

# The U.S. SAFE WEB Act: *The First Three Years*

A Report to Congress

Federal Trade Commission  
December 2009



# **The U.S. SAFE WEB Act:** *The First Three Years*

**A Report to Congress**

December 2009



**Federal Trade Commission**

Jon Leibowitz, Chairman  
Pamela Jones Harbour, Commissioner  
William E. Kovacic, Commissioner  
J. Thomas Rosch, Commissioner

# Table of Contents

Executive Summary .....	i
I. Introduction .....	1
II. History of the U.S. SAFE WEB Act .....	2
III. Overview of the U.S. SAFE WEB Act .....	3
IV. U.S. SAFE WEB Act Reporting Requirements: The First Three Years .....	4
A. Cross-Border Complaints .....	5
B. Sharing of Non-Public Information With Foreign Agencies .....	7
C. Investigative Assistance to Foreign Law Enforcement Agencies .....	12
D. International Agreements .....	14
E. Delayed Notice of Process .....	14
F. Voluntary Provision of Information .....	15
G. Foreign Litigation .....	16
H. Other Provisions .....	17
V. Legislative Recommendation .....	19
VI. Conclusion .....	21
Endnotes .....	22
Appendix A: U.S. SAFE WEB Act Requests Resulting in Enforcement Actions or Ongoing Investigations .....	A-1
Appendix B: FTC Enforcement Actions With Public Cross-Border Components .....	B-1

## Executive Summary

In December 2006, Congress recognized the increasing threats facing U.S. consumers in the global marketplace from the proliferation of spam, spyware, telemarketing, and other cross-border fraud and passed the Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006 (“U.S. SAFE WEB Act,” “SAFE WEB,” or “Act”). The Act enhances the ability of the Federal Trade Commission (“FTC”) to protect consumers from significant economic injury and other harm by giving the agency new or expanded powers in several key areas. With the authority granted by the Act, the FTC has shared information in response to **38** requests from **14** foreign law enforcement agencies, resulting in over **17** enforcement actions by U.S. and foreign authorities, and issued **23** civil investigative demands on behalf of **6** foreign agencies in **11** investigations. The FTC has obtained formal negotiating authority and shared draft text of international agreements with key foreign partners, asserted its cross-border jurisdictional and remedial authority in legal briefs to defend against spurious challenges, and hosted **23** foreign officials from **14** countries in its new International Fellows Program and SAFE WEB Interns Program. Through their work, Fellows have facilitated investigations of foreign operations targeting U.S. consumers and otherwise strengthened FTC enforcement teams. In short, the FTC has used the new authority to further the goals set forth in the Act—protecting American consumers from cross-border harm.

The FTC submits this report to Congress pursuant to section 14 of the U.S. SAFE WEB Act. Section 14 requires the FTC, within three years of the date of enactment, to submit a report to Congress describing its use of and experience with the authority granted by the Act, including:

- (1) the number of cross-border complaints received by the FTC;
- (2) the identification of and results of cooperation with foreign agencies with whom the FTC has shared non-public information under the Act;
- (3) the number of times the FTC has issued compulsory process on behalf of foreign agencies;
- (4) a list of international agreements or memoranda of understanding executed by the FTC that relate to the Act;
- (5) the number of times the FTC has sought delay of notice under the Act and the number of times courts have granted a delay;
- (6) a description of the types of information private entities have provided voluntarily pursuant to the Act and an analysis of whether the lack of a FOIA exemption for such material provided has hindered FTC investigations or enforcement proceedings; and
- (7) a description of FTC litigation brought in foreign courts.

Section 14 also requires the FTC to include in its report any recommendations for additional legislation. Accordingly, the FTC recommends that Congress act now to remove the sunset provision from the Act. Indeed, as this report illustrates, the Act has played a significant role in facilitating cross-border cooperation in investigations and enforcement proceedings. The FTC's ability to protect consumers in a global economy would be significantly hampered if the Act were to expire. The FTC's need for this authority only increases with the expanding global reach of fraud and other malicious activities. Further, the existence of the sunset provision currently impedes the agency's ability to cooperate with foreign partners who are concerned that the FTC's authority in the areas covered by the Act could expire. Thus, the sunset provision providing that the Act will expire in 2013 undermines the FTC's ability to utilize fully the authority granted by the Act now. Given the essential role the Act plays in the FTC's ability to carry out its consumer protection mission, along with the growing need for continued cooperation to combat fraud and deception in the global marketplace, the FTC recommends that Congress take immediate action to repeal the sunset provision.

In this report, the FTC provides information on the items specifically enumerated in the Act and implementation updates on other key provisions of the Act. To prepare this report, the FTC developed internal procedures to track information sharing and investigative assistance pursuant to the Act. The FTC also conducted a comprehensive assessment of the agency's activities conducted pursuant to the Act through formal mechanisms and informal staff questionnaires. In brief, the FTC compiled the following data:

- ❖ **Cross-Border Complaints:** In calendar years 2006 through 2008, the FTC received 97,287, 86,564, and 76,835 cross-border complaints, respectively, submitted to its Consumer Sentinel Network.
- ❖ **Information Sharing:** The FTC has shared compelled or confidential information in response to **38** requests from **14** foreign agencies in **6** countries. In several of these matters, the FTC and the foreign agency both subsequently initiated enforcement proceedings against the investigative targets.
- ❖ **Investigative Assistance:** The FTC has issued **23** civil investigative demands in **11** investigations on behalf of **6** foreign agencies in **4** countries.
- ❖ **International Agreements:** The FTC, with approval from the Department of State, shared draft international SAFE WEB agreements with Canada and the European Commission. In addition, the FTC has initiated formal negotiations with the European Commission.

- ❖ **Delay of Notice:** The FTC has not sought court orders pursuant to the Act seeking to delay notice by the recipient of compulsory process to the investigative target. However, in some instances, third parties who initially indicated that they would notify their customers of the FTC’s compulsory process agreed to withhold notification after FTC staff informed them of this new authority. As a result, the provision has been effective in encouraging voluntary compliance with the FTC’s confidentiality requests.
- ❖ **Voluntary Disclosures:** The FTC has received a variety of information provided voluntarily by private entities, including account information from banks and registration information from domain name registrars.
- ❖ **Foreign Litigation:** The FTC entered into an agreement with the Department of Justice’s Office of Foreign Litigation that designated an FTC attorney to work in the Office of Foreign Litigation. As a result of this agreement, the FTC has worked with foreign counsel to compel the production of evidence in foreign courts to assist the development of FTC cases in domestic proceedings.
- ❖ **International Fellows Program and SAFE WEB Interns Program:** The FTC has hosted **23** foreign officials from **14** countries. These officials have contributed to several enforcement actions, including Operation Tele-PHONEY, a coordinated enforcement sweep against deceptive telemarketers. Indeed, as part of this sweep, a Canadian Fellow played a pivotal role both as an investigator on the FTC’s enforcement team and by facilitating cooperation between the FTC and the Canadian Competition Bureau, including sharing information pursuant to the Act. The Competition Bureau provided reciprocal assistance to the FTC in connection with its enforcement actions. In addition, the Canadian actions that were part of the sweep resulted in criminal charges against four defendants and the conviction of two previously-charged defendants, one of whom pled guilty.

Over the past three years, the FTC has adopted a comprehensive approach in implementing the Act. As part of these efforts, the FTC has integrated the Act’s authority into its investigations and enforcement proceedings. The best illustrations of the use of this authority come from matters involving unlawful spam messages, Internet fraud, and deceptive schemes seeking to take advantage of U.S. consumers during the economic downturn. A few examples are highlighted below.

- ❖ In *FTC v. Atkinson*, the FTC shut down a vast international spam network that peddled bogus prescription drugs, weight-loss pills, and male-enhancement products to U.S. and foreign consumers. In this case, the FTC used the Act’s authority to share non-public

information obtained pursuant to compulsory process with the New Zealand Department of Internal Affairs (NZDIA) and the Australian Communications and Media Authority (ACMA). NZDIA, using the information provided by the FTC, executed multiple search warrants on locations in New Zealand that were affiliated with the operation and provided the FTC with further information about the scheme. The FTC brought an enforcement action and obtained a \$15.15 million default judgment against Atkinson and his company, and a \$3.77 million default judgment against the remaining three corporate defendants. In addition, the FTC obtained a settlement agreement with the remaining individual defendant. The FBI executed search warrants connected to this matter, and one of the defendants in the FTC's action pled guilty to a federal criminal charge. NZDIA filed an enforcement action in New Zealand and obtained settlements with all three of the defendants in its case totaling NZ\$250,000 (approximately US\$179,000).

- ❖ In *FTC v. Cash Today, Ltd.*, the FTC and the State of Nevada filed actions against ten related Internet payday lenders and their principals, based mainly in the United Kingdom, alleging that they engaged in unfair and deceptive collection tactics and failed to make required written disclosures before completing consumer credit transactions with U.S. consumers. During its investigation, the FTC shared non-public information with authorities in the United Kingdom, and the UK Office of Fair Trading provided assistance with the investigation. The FTC obtained a \$1 million settlement agreement with the U.S. and UK defendants that prohibits them from engaging in deceptive lending and collection practices.

The FTC has also used the Act's authority to provide investigative assistance to foreign law enforcement agencies, which in some instances, are investigating foreign operations that also target U.S. consumers.

- ❖ For example, the FTC issued a civil investigative demand to a U.S. company on behalf of the Toronto Police Service to obtain account information associated with alleged Canada-based scams that harmed both U.S. and Canadian consumers. With the information obtained by the FTC, the Toronto Police Service was able to link one of the suspects to the scam, and it subsequently arrested the suspect, along with the 13 other individuals involved in the fraudulent operation.

As these examples demonstrate, the FTC has used the Act's authority quickly and effectively to protect consumers in the global economy. The Act has helped the FTC to 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. Indeed, as malefactors continue to exploit new technologies to defraud consumers, the FTC will increasingly rely on the Act's authority to shut down fraudulent operations and protect consumers. The FTC therefore recommends that Congress preserve this much-needed authority and repeal the sunset provision in the Act.



## I. Introduction

*Imagine the following scenario:*

*The Federal Trade Commission (“FTC”) obtains a court order against a spammer defrauding U.S. consumers by selling bogus miracle cures. The order shuts down the spammer’s websites. The FTC then learns that the spammer has an affiliate that is perpetrating the same scam from Australia. Despite the FTC’s lawsuit, U.S. consumers and foreign consumers continue to be bombarded by this spam. The Australian authority prepares to take action against the affiliate, and asks the FTC for investigative information to help its law enforcement efforts.*

*Before the passage of the U.S. SAFE WEB Act,<sup>1</sup> the FTC could not have shared the evidence it obtained using its main investigatory tool, the civil investigative demand, with the Australian agency. Now, with the U.S. SAFE WEB Act, the FTC can share the information from its own investigation with the Australian authority to support an Australian action against the affiliate spammer. The FTC can also send a civil investigative demand on behalf of the Australian authority to the U.S.-based ISP that hosts some of the affiliate’s websites. This evidence helps the Australian authority shut down the affiliate’s websites and benefits U.S. consumers.*

In December 2006, Congress recognized the increasing threats facing U.S. consumers in the global marketplace from the proliferation of spam, spyware, telemarketing, and other cross-border fraud and passed the U.S. SAFE WEB Act. The Act enhances the FTC’s ability to protect consumers from significant economic injury and other harm. Indeed, the Act provides the FTC with a broad range of powerful tools and strengthens the FTC’s authority in five key areas: (1) information sharing; (2) investigative assistance; (3) confidentiality; (4) enhanced investigative and litigating tools; and (5) enforcement relationships.

The FTC submits this report pursuant to section 14 of the Act, which requires the FTC to issue a report to Congress within three years of the date of enactment that provides information on the agency’s use of and experience with the Act, and includes any recommendations for additional legislation.<sup>2</sup> Sections II and III of the report provide historical background and an overview of the Act. Section IV sets forth detailed information corresponding to the Act’s reporting requirements.

Since the passage of the Act, the FTC has used this new authority effectively in its investigations and enforcement proceedings, particularly in cross-border cases. Thus, Section V includes a legislative recommendation that Congress take immediate action to repeal the Act’s sunset provision. As the report demonstrates, the Act has played a significant role in facilitating cross-border cooperation in the FTC’s investigations and enforcement proceedings. In light of the essential role the Act plays in the FTC’s ability to carry out its mission, along with the growing need for continued cooperation to combat new and existing global threats to U.S. consumers, the FTC recommends that Congress repeal the sunset provision now.

## II. History of the U.S. SAFE WEB Act

Near the end of the last century, globalization of trade, improvements in international telecommunications, and the advent of the Internet created unprecedented new opportunities for consumers and businesses, but also posed novel and difficult challenges. In separate appearances before three Congressional committees in 2001, the FTC described the nature of the problems facing American consumers—and U.S. law enforcement—from Internet and telemarketing scams by foreign fraud operators.<sup>3</sup> The problems ranged from traditional scams that thrived online, such as pyramid schemes and business operations making false product claims, to aggressive advance-fee loan, foreign lottery, and sweepstakes telemarketing schemes to Internet-enabled frauds like modem hijacking.

The FTC's testimony highlighted the rapid growth of fraudulent and deceptive cross-border marketing scams aimed at American consumers at the beginning of the century. In 1995, less than 1% of all complaints to the FTC involved foreign consumers complaining about domestic businesses or domestic consumers complaining about foreign businesses. By 2001, the percentage of those complaints in the FTC's Consumer Sentinel Network had risen to 12%.<sup>4</sup>

To combat increasing cross-border fraud, the FTC worked to improve its enforcement cooperation with foreign counterparts in international organizations and regional partnerships. The FTC recognized the challenges cross-border schemes create for law enforcement, including the global reach and instantaneous speed of the Internet and the ability of scammers to cloak themselves in anonymity. The FTC also identified roadblocks created by national borders and domestic laws, such as the inability to share information with foreign law enforcers about targets located in the foreign country. Many of these challenges reflected the shortcomings of a legal framework developed when consumer protection was an almost purely domestic concern. Accordingly, the FTC worked with Congress to explore how the “existing legal framework for sharing information might be modified to facilitate cooperation in cross-border cases,” and how to make the agency's civil remedies more effective across borders.<sup>5</sup>

In June 2005, the FTC sent a legislative recommendation to Congress for the “Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2005” to strengthen the FTC's ability to fight cross-border fraud.<sup>6</sup> The FTC also submitted a report to Congress that provided a detailed picture of cross-border fraud and the types of harms its victims experienced.<sup>7</sup> The legislative recommendations were based on the FTC's experiences in its cross-border investigations and cases, on the international consensus reflected in the Organization for Economic Cooperation and Development's 2003 “Guidelines for Protecting Consumers Across Borders from Fraudulent and Deceptive Commercial Practices,”<sup>8</sup> and the

experience of other federal agencies, such as the Securities and Exchange Commission, that had already been granted similar authority to address cross-border issues.<sup>9</sup> The FTC and interested stakeholders from industry and consumer organizations worked with Congress to facilitate consideration of the legislative recommendation. On December 8, 2006, Congress passed the U.S. SAFE WEB Act.<sup>10</sup> It was signed into law on December 22, 2006.<sup>11</sup>

### III. Overview of the U.S. SAFE WEB Act

The Act strengthens the FTC’s authority in five key areas: (1) information sharing; (2) investigative assistance; (3) confidentiality; (4) enhanced investigative and litigating tools; and (5) enforcement relationships. First, the Act authorizes the FTC, in appropriate consumer protection matters, to share compelled and confidential information with foreign law enforcement agencies.<sup>12</sup> Before the Act was passed, the FTC could only share such information with other U.S. enforcers—not with foreign enforcers. Now, the FTC can exercise its discretion to share this information with its foreign law enforcement counterparts, as long as certain statutory factors are satisfied.

Second, the Act permits the FTC to provide investigative assistance in consumer protection matters to foreign law enforcement agencies.<sup>13</sup> If the FTC determines that the requested cooperation is consistent with the requirements in the Act, it can issue compulsory process for documents and testimony to an entity located in the United States and share the information with the foreign agency.<sup>14</sup> Before the Act was passed, the FTC could not provide such assistance to a foreign agency—even if the foreign agency’s investigation would ultimately benefit U.S. consumers. The Act also authorizes the FTC to initiate a proceeding under an existing federal statute to obtain testimony, documents, or things for use in foreign or international proceedings.<sup>15</sup>

Third, the Act enables the FTC to obtain information it would not otherwise receive from foreign entities that were previously concerned about public disclosure of their information. If the foreign agency or source requests confidential treatment as a condition of providing the information, the Act authorizes the FTC to protect the confidentiality of: (1) information that a foreign government agency provides to the FTC; or (2) any material reflecting a consumer complaint obtained from a foreign source.<sup>16</sup> In addition, the Act exempts from public disclosure consumer complaints submitted to a Commission reporting mechanism sponsored in part by other foreign agencies.<sup>17</sup> The Act includes a limited exception for disclosure when necessary to comply with a court order or Congressional request.<sup>18</sup>

Fourth, the Act provides enhanced investigative and litigating tools for both domestic and cross-border cases. For example, the Act authorizes the FTC to request a court order seeking delay of notice by the recipient of compulsory process to the investigative target when notice would otherwise cause an adverse result.<sup>19</sup> In addition, the Act exempts certain private entities from liability for providing information voluntarily to the FTC.<sup>20</sup> With respect to cross-border litigation, the Act clarifies the scope of the FTC's cross-border jurisdiction and remedial authority.<sup>21</sup> The Act also authorizes the FTC to assist the Attorney General in connection with litigation in foreign courts on relevant matters.<sup>22</sup>

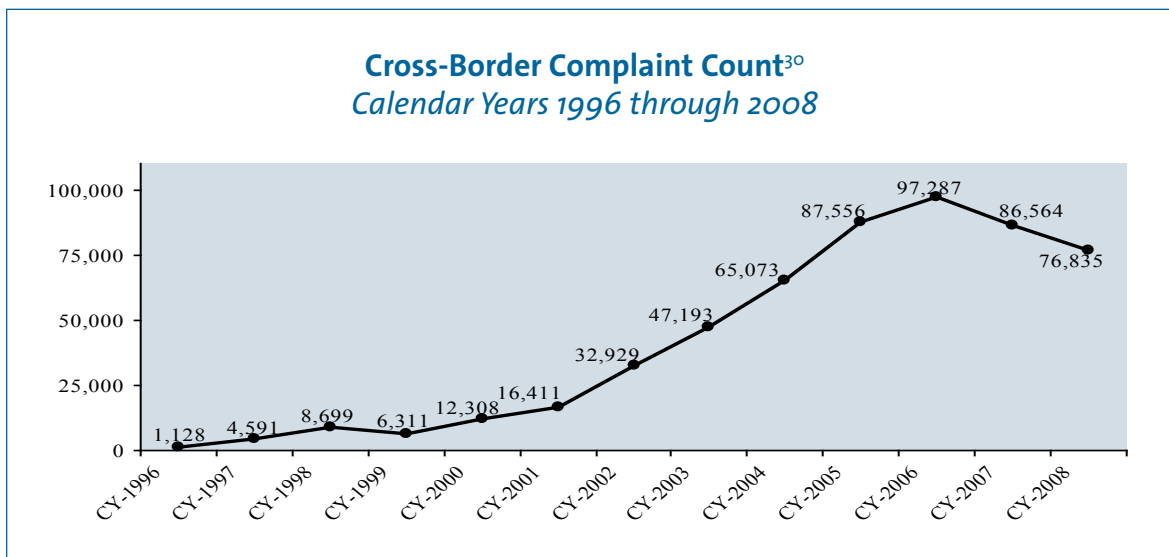
Finally, the Act contains several provisions aimed at strengthening the FTC's enforcement relationships with foreign agencies. For example, the Act allows the FTC to participate in staff exchanges with foreign agencies.<sup>23</sup> In addition, the Act permits the FTC, with the approval of the Department of State, to enter into binding international consumer protection agreements when such agreements are required as a condition for providing information or reciprocal assistance.<sup>24</sup>

#### **IV. U.S. SAFE WEB Act Reporting Requirements: The First Three Years**

The Act requires the FTC to issue a report to Congress within three years of enactment that includes any recommendations for additional legislation and provides information on its use and experience with the Act, including: (1) the number of cross-border complaints received by the FTC; (2) the identification of and results of cooperation with foreign agencies with whom the FTC has shared non-public information under the Act; (3) the number of times the FTC has issued compulsory process on behalf of foreign agencies; (4) a list of international agreements or memoranda of understanding executed by the FTC that relate to the Act; (5) the number of times the FTC has sought delay of notice under the Act and the number of times courts have granted a delay; (6) a description of the types of information private entities have provided voluntarily pursuant to the Act and an analysis of whether the lack of a FOIA exemption for material provided has hindered FTC investigations or enforcement proceedings; and (7) a description of FTC litigation brought in foreign courts.<sup>25</sup> This section sets forth the reporting information required by the Act.

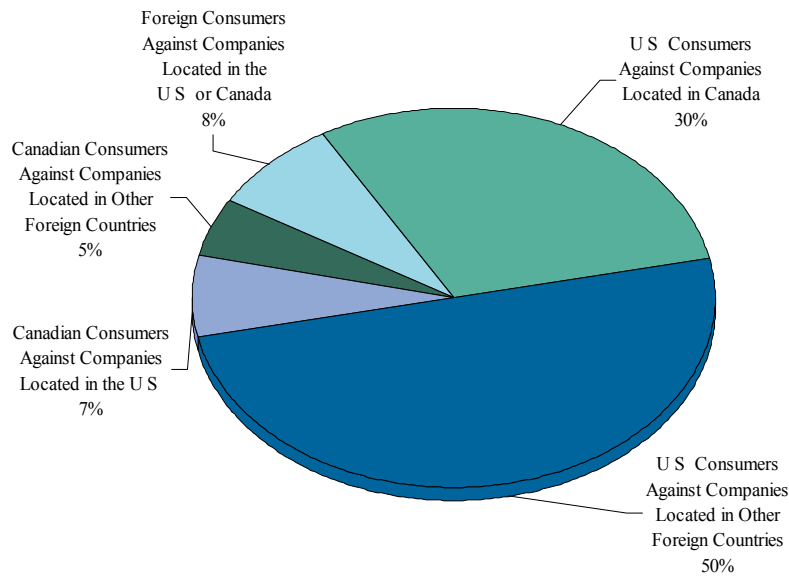
## A. Cross-Border Complaints

In calendar years 2006 through 2008, the FTC’s Consumer Sentinel Network received 97,287, 86,564, and 76,835 cross-border complaints, respectively, from U.S. and foreign consumers.<sup>26</sup> Cross-border complaints comprised 23%, 15%, and 12% of all fraud complaints received from 2006-2008, respectively.<sup>27</sup> (The Consumer Sentinel Network relies on information from several different data contributors, so the decrease in reported complaints is not attributable to any single factor.) In the past three years, American consumer complaints against foreign businesses have accounted for roughly four out of five cross-border complaints.<sup>28</sup> Indeed, of all cross-border fraud complaints in calendar year 2008 (76,835), 30% (22,806) were from U.S. consumers complaining about Canadian companies while 50% (38,684) were from U.S. consumers complaining about other foreign companies (the remaining complaints were from foreign consumers).<sup>29</sup> These numbers may understate the extent of cross-border fraud: In many instances, consumers submitting complaints do not identify a foreign component because they are not aware that a foreign entity may be involved, particularly because many foreign con artists conceal their location by using U.S.-based postal addresses, VoIP phone technology, and the Internet.



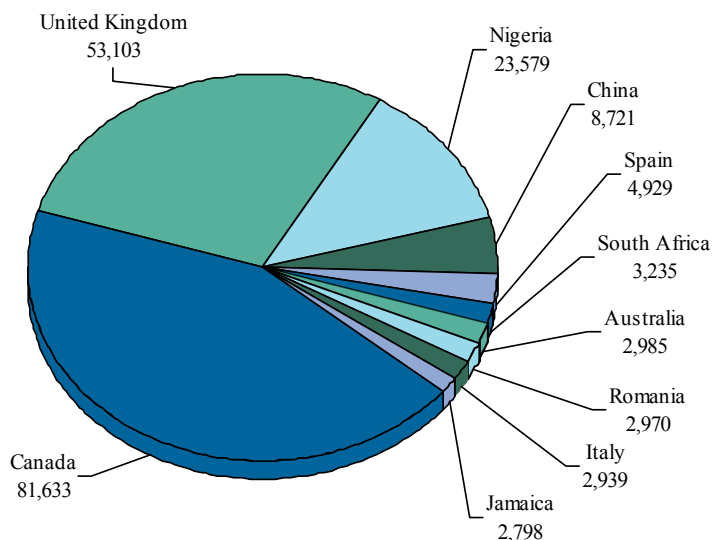
During the period January 1, 2007-June 30, 2009, the consumer complaints in the Consumer Sentinel Network identified companies with connections to over 200 countries. The top 10 country locations for foreign companies identified in consumer complaints were Canada, the United Kingdom, Nigeria, China, Spain, South Africa, Australia, Romania, Italy, and Jamaica, respectively. In many instances, however, foreign companies fail to disclose their accurate location, so the actual location of the companies responsible for the reported fraud could vary.

**Cross-Border Fraud Complaints By Consumer and Company Location<sup>31</sup>**  
*January 1 – December 31, 2008*



Interestingly, the most common method of communication by companies outside of the U.S. and Canada targeting U.S. consumers was email.<sup>32</sup> Specifically, 84%, 83%, and 80% of consumers who reported the method of contact were contacted via email from 2006 to 2008, respectively.<sup>33</sup> In 2008, prizes and sweepstakes scams were the largest category of reported cross-border fraud.<sup>34</sup>

**Top 10 Foreign Company Locations**  
*January 1, 2007 – June 30, 2009*



The reported economic loss resulting from cross-border fraud is significant. In 2006, the total injury reported to the Consumer Sentinel Network by U.S. consumers in complaints against foreign companies was \$218,860,966.<sup>35</sup> In 2007, the amount increased to \$271,178,951.<sup>36</sup> In 2008, the reported injury was \$214,286,621.<sup>37</sup> However, as previously noted, these annual totals likely understate the total amount of loss because many consumers do not submit complaints and, even if they do so, they do not always report the amount of loss.

## B. Sharing of Non-Public Information With Foreign Agencies

Sections 4(a) and 6(a) of the Act grant the FTC authority to share certain confidential and compelled information in consumer protection investigations with foreign law enforcement agencies.<sup>38</sup> Before the Act was passed, the FTC could only share this information with U.S. enforcers—not foreign enforcers. The information sharing authority is implemented in Commission Rule 4.11(j), which sets forth internal agency procedures for handling requests from foreign law enforcement agencies.<sup>39</sup> The new rule generally adopts the procedures of Rule 4.11(c), relating to the sharing of information with federal and state law enforcement agencies, and incorporates the requirements and restrictions of the Act.<sup>40</sup> Rule 4.11(j) applies to material submitted to the FTC on or after December 22, 2006, the date the Act became law.<sup>41</sup>

The Act requires the foreign agency to provide assurances that the information will be maintained in confidence. In addition, the agency must provide assurances that the information will be used only for investigating or engaging in enforcement proceedings against possible violations of foreign laws prohibiting fraudulent or deceptive commercial practices, or other practices substantially similar to practices prohibited by any law administered by the FTC (except antitrust laws, which are not covered by this provision). If these conditions are met, the FTC can now exercise its discretion to disclose compelled or confidential information.<sup>42</sup>

The information sharing authority has helped to streamline parallel investigations and avoid duplication of efforts. It has also increased the quantity and improved the quality of evidence against common targets. Indeed, enhanced cooperation with foreign authorities strengthens the FTC's ability to protect U.S. consumers. The FTC has used its authority to share compelled and confidential information with **14** foreign agencies from **6** countries in response to **38** requests in cross-border consumer protection matters, including fraudulent telemarketing scams, deceptive mail schemes, and spam cases. A list of information sharing and investigative assistance requests made pursuant to the Act that resulted in enforcement proceedings or ongoing investigations with notable developments is included in Appendix A.

The FTC has shared non-public information pursuant to the Act with the following agencies:

<b>Name of Agency</b>	<b>Country</b>
Australian Communications and Media Authority	Australia
Canadian Radio-television and Telecommunications Commission	Canada
Competition Bureau Canada	Canada
Edmonton Police Service	Canada
Ministry of the Attorney General (Ontario)	Canada
Office of the Privacy Commissioner	Canada
Ontario Provincial Police	Canada
Royal Canadian Mounted Police	Canada
Toronto Police Service	Canada
Independent Post and Telecommunications Authority (OPTA)	The Netherlands
Department of Internal Affairs	New Zealand
City of London Police	United Kingdom
Office of Fair Trading	United Kingdom
Security Service of Ukraine	Ukraine

The FTC has used the Act’s information sharing authority in a substantial number of cross-border investigations and enforcement actions to crack down on global scams injuring U.S. and foreign consumers. In particular, consistent with the underlying purposes of the Act, the FTC has filed several cross-border cases involving spam and spyware. In addition, since the passage of the Act, the FTC has brought a number of cases against scam artists seeking to take advantage of consumers during the economic downturn. A few examples are highlighted below.<sup>43</sup>



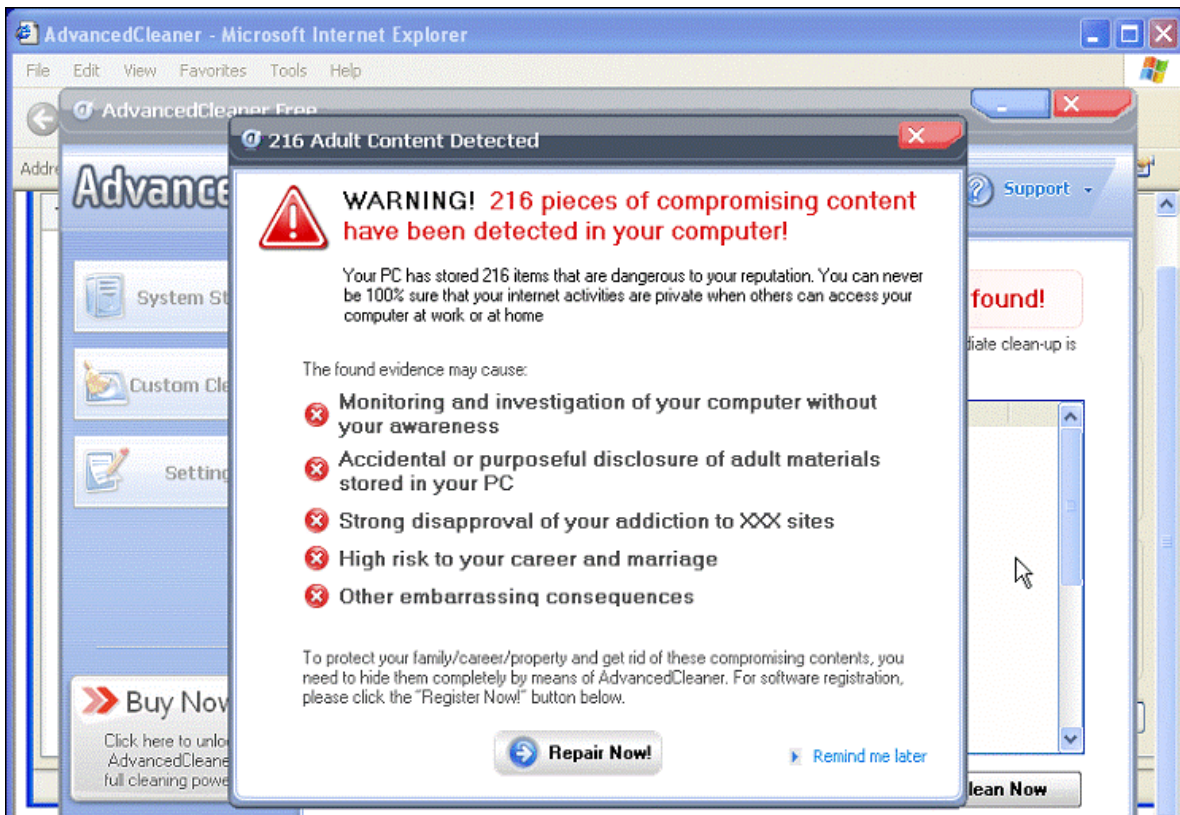
## **FTC SHUTS DOWN VAST INTERNATIONAL SPAM NETWORK USING THE U.S. SAFE WEB ACT**

In *FTC v. Atkinson*, the FTC shut down a vast international spam network that peddled bogus prescription drugs, weight-loss pills, and male-enhancement products through billions of spam emails sent to U.S. and foreign consumers. In this case, the FTC shared non-public information obtained pursuant to compulsory process with the New Zealand Department of Internal Affairs (NZDIA) and the Australian Communications and Media Authority (ACMA). Spamhaus, a well-known anti-spam organization, identified the network as the largest “spam gang” in the world. The FTC received more than three million complaints about spam messages connected to this operation. NZDIA, using the information provided by the FTC, executed multiple search warrants on locations in New Zealand that were affiliated with the operation and subsequently shared information with the FTC. The FTC filed an enforcement action against Lance Atkinson, a New Zealand citizen living in Australia, and others affiliated with the case. The FTC obtained a \$15.15 million default judgment against Atkinson and his company, and a \$3.77 million default judgment against the remaining three corporate defendants. In addition, the FTC obtained a settlement agreement with the remaining individual defendant. The FBI simultaneously executed search warrants connected to this matter, and one of the defendants in the FTC’s action pled guilty to a federal criminal charge. NZDIA brought an enforcement action in New Zealand and obtained settlements with all three of the defendants in its case totaling NZ\$250,000 (approximately US\$179,000).

The *Atkinson* case illustrates precisely what the Act was intended to achieve. In this complex investigation, the Act provided the FTC with the authority to share meaningful information with multiple foreign agencies in the countries where the targets of the investigation were operating. With this information, the authorities volunteered to provide reciprocal information, which the FTC used in its own investigation to protect U.S. consumers. The Act facilitated global cooperation that was essential to shut down an international spam network that spanned several countries.

## FTC HALTS MASSIVE DECEPTIVE “SCAREWARE” ADVERTISING SCHEME

In *FTC v. Innovative Marketing, Inc.*, the FTC filed an action to stop a massive “scareware” scheme, which relied on purportedly bogus computer scans to detect viruses, spyware, and illegal pornography on consumers’ computers. The scheme allegedly tricked more than one million U.S. and foreign consumers into buying fraudulent computer security products and generated more than \$100 million in revenues. The FTC alleged that the defendants disseminated their fake computer scans by inserting hidden code into seemingly legitimate Internet advertisements. Once this hidden code was activated, consumers were redirected from the website they were viewing to one of the defendants’ websites, where the fake scan commenced. One of the corporate defendants in the suit was a Belize company with its principal office in Kiev, Ukraine. The FTC shared information pursuant to the Act with Canadian authorities, which subsequently assisted the FTC with its investigation. The FTC has obtained entries of default against two of the defendants and settled with two other defendants, requiring them to forfeit over \$100,000 of assets and prohibiting them from using deceptive “scareware” advertising practices and installing malicious programs onto consumers’ computers. The case is still pending with respect to the remaining defendants. The graphic below is an example of one of the deceptive computer warnings that the defendants displayed in this scheme.



The FTC has also targeted scam artists taking advantage of vulnerable U.S. consumers during the economic downturn by launching several enforcement actions as part of Operation Short Change. In one of these cases, *FTC v. MCS Programs, LLC*,<sup>44</sup> the FTC used its SAFE WEB authority to share information with a Canadian agency. In addition, another Canadian authority provided assistance in this case by conducting witness interviews. The FTC alleged that the defendants used telemarketing robocalls and the Internet to convince U.S. and Canadian consumers to pay them \$690 to \$899 for a “rapid debt reduction” program that would purportedly enable them to pay off their debt three to five times faster than they could under their current payment schedule. The FTC obtained an injunction halting the defendants’ scheme and continues to litigate this matter.

### ***FTC HALTS ABUSIVE AND DECEPTIVE DEBT COLLECTION PRACTICES***

In *FTC v. Cash Today, Ltd.*, the FTC and the State of Nevada filed actions against ten related Internet payday lenders and their principals, based mainly in the United Kingdom, alleging violations of the FTC Act by using unfair and deceptive collection tactics. The FTC also alleged that the defendants violated the Truth in Lending Act and Regulation Z by failing to make required written disclosures before completing consumer credit transactions with U.S. consumers. The defendants allegedly provided consumers with payday loans without disclosing any key loan terms in writing, including the annual percentage rate, the payment schedule, the amount financed, the total number of payments, and any late payment fees. The FTC alleged that defendants falsely claimed that consumers were legally obligated to repay the loans and threatened consumers with arrest and imprisonment. During its investigation, the FTC shared non-public information with authorities in the United Kingdom. The UK’s Office of Fair Trading assisted the FTC by obtaining corporate records for the foreign defendants and providing a declaration regarding those records, which the FTC filed in court. The FTC obtained a \$1 million settlement agreement with the U.S. and UK defendants that prohibits them from engaging in deceptive lending and collection practices.

The FTC has also used the Act's information sharing authority to stop economic loss resulting from prize and sweepstakes scams, which, as mentioned in Section IV.A., was the largest category of cross-border fraud reported to the Consumer Sentinel Network in 2008. For example, in *FTC v. B.C. Ltd. 0763496*,<sup>45</sup> the FTC obtained a permanent injunction and \$1 million default judgment against operators of a lottery and prize-promotion scam that used counterfeit checks and false promises of substantial cash prizes to bilk consumers out of large sums of money. In some instances, consumers lost as much as \$24,000 in payments for bogus fees that the scammers charged to retrieve alleged prize winnings. The principal operators of the prize promotion scam resided in Canada. As a result, the FTC used the Act to share key information with Canadian authorities, which brought a related enforcement proceeding against the principals. Canadian authorities arrested one of the principal defendants, who fled to another country after being released on bail. Law enforcement authorities continue to pursue the matter.

As these examples illustrate, the authority to share compelled and confidential information with foreign law enforcement agencies has significantly improved the FTC's ability to engage in mutually beneficial cooperation with foreign partners and bring successful cross-border enforcement actions. Indeed, during the period FY2007-2009, the FTC received assistance from foreign agencies at least 26 times. The cases highlighted above are merely a snapshot of the FTC's cross-border cases. A list of over 40 FTC consumer protection cases with public cross-border components filed in the last three years, many of which involved the use of the Act's authority, is included in Appendix B.

### **C. Investigative Assistance to Foreign Law Enforcement Agencies**

The Act authorizes the FTC to provide investigative assistance to foreign law enforcement agencies. Specifically, section 4(b) of the Act authorizes the Commission, in response to a written request for assistance from a foreign law enforcement agency, to “conduct such investigation as the Commission deems necessary to collect information and evidence pertinent to the request for assistance, using all investigative powers authorized by [the FTC Act].”<sup>46</sup> This provision authorizes the FTC to issue compulsory process, typically civil investigative demands, on behalf of a foreign law enforcement agency.

The Act requires the foreign law enforcement agency to provide assurances that the information will be used for investigating or engaging in enforcement proceedings against possible violations of foreign laws prohibiting fraudulent or deceptive commercial practices, or other practices substantially similar to practices prohibited by any law administered by the FTC (except antitrust laws, which are not covered by the investigative assistance provision). In addition, before the FTC can provide assistance, the Act requires the FTC to consider whether:

(1) the foreign agency would provide reciprocal assistance to the Commission; (2) the use of the FTC’s investigative powers would prejudice the public interest; and (3) the foreign agency’s investigation involves practices that have caused injury or are likely to cause injury to a significant number of persons.

The FTC has used its investigative assistance authority to issue **23** civil investigative demands in **11** investigations on behalf of **6** foreign agencies in **4** countries.<sup>47</sup> The FTC issued compulsory process on behalf of the following agencies:

<b>Name of Agency</b>	<b>Country</b>
Australian Communications and Media Authority	Australia
Competition Bureau Canada	Canada
Edmonton Police Service	Canada
Toronto Police Service	Canada
Independent Post and Telecommunications Authority (OPTA)	The Netherlands
Department of Internal Affairs	New Zealand

The nature of these requests has varied. In some matters, the FTC has issued compulsory process to domain name registrars and email service providers in connection with foreign spam investigations. In other instances, the FTC has issued compulsory process to telephone service providers in connection with foreign telemarketing schemes. In each of these requests, the FTC carefully weighed the factors outlined in the Act and shared the information with the foreign agencies pursuant to the Act’s information sharing provisions.

A few examples of the FTC’s use of the Act’s investigative assistance authority are highlighted below.

- ❖ The FTC issued a civil investigative demand to a U.S. company on behalf of the Toronto Police Service (TPS) to obtain account information associated with alleged Canadian-based scams that harmed both U.S. and Canadian consumers. With the information obtained by the FTC, the TPS was able to link one of the suspects to the scam, and it subsequently arrested the suspect, along with the 13 other individuals involved in the fraudulent operation.
- ❖ The FTC issued a civil investigative demand to a U.S. domain name registrar on behalf of The Netherlands Independent Post and Telecommunications Authority (OPTA), the Dutch agency that enforces anti-spam laws. OPTA used the information provided by

the FTC to confirm the identity of the suspect allegedly involved in the spam operation and was able to proceed with its investigation.

- ❖ The TPS arrested a suspect who allegedly engaged in fraudulent telemarketing schemes and, as part of its investigation, the TPS submitted a request to the FTC to obtain information from a U.S.-based telephone company about an account associated with the suspect. The information obtained by the FTC helped the TPS identify U.S. victims of the Canadian suspect's scam. The TPS continues to pursue this matter.

Section 4(b) of the Act also authorizes the FTC to initiate proceedings pursuant to 28 U.S.C. § 1782 on behalf of foreign agencies to obtain testimony, documents, or things for use in foreign proceedings.<sup>48</sup> To date, the FTC has not had the occasion to initiate such a proceeding because the investigative assistance requests it has received have related only to the issuance of compulsory process at the investigative stage. However, the FTC often seeks assistance in acquiring similar foreign evidence in its cross-border cases. As a result, the FTC intends to invoke this authority in the future, when appropriate, to encourage reciprocal assistance.

#### **D. International Agreements**

Section 4(b) of the Act authorizes the Commission, with the prior approval and ongoing oversight of the Secretary of State, to enter into binding international agreements for mutual legal assistance in consumer protection matters.<sup>49</sup> Pursuant to this provision, and the provisions implementing the Case-Zablocki Act,<sup>50</sup> the FTC has worked closely with the Department of State to pursue international agreements with Canada and with the European Commission.<sup>51</sup>

In 2007, the FTC obtained approval from the Department of State to begin formal negotiations and in 2008, the Department of State cleared draft agreements to be shared with Canada and the European Commission. Since that time, the FTC delivered the draft text and has held a series of background discussions with its European and Canadian colleagues. In May 2009, the European Commission received formal negotiating authority, and it has actively been negotiating the terms of an agreement. In the year ahead, the FTC plans to continue negotiations to finalize a European agreement and pursue formal negotiations with Canadian partners.

#### **E. Delayed Notice of Process**

Section 7 of the Act authorizes the FTC to seek an *ex parte* court order, and extensions of such an order, delaying notice of process to the investigative target in consumer protection investigations if the FTC believes that notification will cause an adverse result.<sup>52</sup> An “adverse result” includes the endangerment of life or physical safety; flight from prosecution; destruction

of, or tampering with, evidence; the intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or proceeding related to fraudulent or deceptive practices.<sup>53</sup> The FTC may use procedures for delayed notification outlined in the Right to Financial Privacy Act, 12 U.S.C. §§ 3401 *et seq.*, and the Electronic Communications Privacy Act, 18 U.S.C. § 2705, if applicable. Otherwise, the FTC will follow the procedures prescribed in the Act to seek the court order.

The FTC has carefully considered whether it should invoke this authority to seek an order delaying notice of process in a number of cases. The FTC has not yet sought a court order under this provision and is currently evaluating whether it will initiate proceedings under this provision in pending cases. The FTC carefully weighs this decision in each case where use of the authority would be appropriate, and there are certainly circumstances in which use of the delayed notice procedure would be considered a viable option. It has not been necessary to exercise this authority because some parties who had initially indicated that they would notify their customers of the FTC's compulsory process agreed to withhold notification after FTC staff notified them of this new authority. As a result, the provision has encouraged voluntary compliance with the FTC's confidentiality requests.

## **F. Voluntary Provision of Information**

Section 8 of the Act exempts certain specified entities from liability for disclosing to the Commission information that may help to reveal unlawful conduct.<sup>54</sup> Private sector representatives who were concerned about providing information voluntarily to the FTC advocated for the inclusion of this provision, which is modeled on a “safe harbor” provision for reporting illegal activities to financial institutions.<sup>55</sup> Specifically, section 8 provides that “financial institutions” are exempt from liability for disclosing assets or suspicious chargeback rates related to possible deceptive or fraudulent commercial practices, assets related to persons involved in such practices, or assets recoverable by the Commission.<sup>56</sup> Section 8 states that, to the extent they are not “financial institutions,” certain other entities that provide financial services, and certain other described entities, such as domain name registrars, are exempt from liability for providing (or failing to provide notice for providing) material that the entities reasonably believe is relevant to possible violations of section 5 of the FTC Act, or assets subject to recovery by the Commission.<sup>57</sup> Section 8 further provides that an Internet service provider (ISP) or provider of telephone services is exempt from liability for providing (or failing to provide notice for providing) “consumer complaints sent to it, or information contained therein.”<sup>58</sup>

Since the Act became law, entities covered by the above exemptions have provided information voluntarily to the FTC. For example, banks have provided account information for targets; domain name registrars have provided domain name registration records for targets; and ISPs have voluntarily searched for consumer complaints about targets. The FTC has used bank records provided by companies voluntarily to assess the chargeback rates of targets, the magnitude of consumer injury caused by targets’ deceptive practices, and trace the assets of targets. FTC staff used information provided by a foreign domain name registrar to identify subscriber information for certain Internet protocol addresses and payment information about targets. Through this voluntary cooperation, section 8 of the Act has assisted the FTC in investigating deceptive or unfair conduct.

Section 14(8) of the Act also requires the FTC’s report to Congress to include “an analysis of whether the lack of an exemption from the disclosure requirements of section 552 of title 5, United States Code [Freedom of Information Act, or “FOIA”], with regard to information or material voluntarily provided relevant to possible unfair or deceptive acts or practices, has hindered the Commission in investigating or engaging in enforcement proceedings against such practices.”<sup>59</sup> The FTC is not aware of any entity that has declined to share information voluntarily specifically because of a FOIA exemption. The FTC, however, has experienced entities first being willing to disclose information, and then failing to do so for different reasons. It is very difficult to determine when such instances involve concerns about later public disclosure of the information provided.

## G. Foreign Litigation

Section 5 of the U.S. SAFE WEB Act authorizes the FTC, with the concurrence of the Attorney General, to designate one or more FTC attorneys to work with the Department of Justice on “litigation in foreign courts on particular matters in which the Commission has an interest.”<sup>60</sup> Pursuant to this provision and 28 U.S.C. § 515,<sup>61</sup> the FTC and the Department of Justice entered into a Memorandum of Understanding (MOU) in late 2008 whereby an FTC attorney was designated a “Special Attorney” in the Department of Justice’s Office of Foreign Litigation (“OFL”). This attorney has been working at OFL on a part-time basis.





Under the MOU, the FTC and OFL have worked closely on a number of matters. In FTC enforcement actions in which the defendants have hidden their assets offshore, the FTC and OFL have retained foreign counsel to assist with requests to foreign courts for international judicial assistance to locate those assets and uncover evidence that can be used in the FTC’s domestic proceedings. For example, in *FTC v. Data Business Solutions, Inc.*, a case involving purportedly bogus domain name registration invoices sent to consumers and small businesses,<sup>62</sup> the defendants deposited their alleged ill-gotten gains in Canadian bank accounts, and they used third-party mailing and printing services located in Canada and the Bahamas. The FTC worked with OFL and retained foreign counsel who filed an application in a Canadian court to compel the production of evidence that will be used in the FTC’s domestic proceedings against these defendants. The FTC and OFL continue to work closely to identify appropriate cases for foreign litigation to obtain evidence and secure assets for consumer redress, in Canada as well as other foreign jurisdictions.

## H. Other Provisions

In addition to the aforementioned items, there has been significant progress with respect to the implementation of several other provisions in the Act. Specifically, the use of the staff exchange and cross-border remedial authority provisions is highlighted below.

### 1. Staff Exchanges

Section 9 of 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” under section 2 of the FTC Act, or under sections 3101 (general authority to employ) or 3109 (temporary or intermittent employment of experts and consultants) of Title 5.<sup>63</sup> To implement this provision, the FTC created an International Fellows Program and a SAFE WEB Interns Program, inviting **23** foreign colleagues from **14** countries to spend up to six months at the FTC.<sup>64</sup> Foreign participants have included an advisor to a commissioner at a foreign agency, a senior investigator, a senior prosecutor, and an attorney/economist who returned to her home agency to lead its consumer protection program.

In many instances, the Fellows have facilitated investigations into fraudulent and deceptive practices or other unlawful conduct. For example, in the FTC’s 2008 telemarketing sweep, Operation Tele-PHONEY, a Canadian Fellow played a pivotal role in the sweep both as an investigator on the FTC’s enforcement team and by facilitating cooperation between the FTC and Canadian Competition Bureau, including sharing information pursuant to the Act. The Competition Bureau assisted the FTC with its enforcement actions. The Canadian actions

resulted in criminal charges against four defendants and the conviction of two previously-charged defendants, one of whom pled guilty. In addition, Fellows from the New Brunswick Office of the Attorney General, the Australian Competition and Consumer Commission, and the Canadian Office of the Privacy Commissioner have all provided substantial assistance in cross-border consumer protection cases, including facilitating information sharing and recovery of foreign assets for consumer redress.<sup>65</sup>

## **2. Cross-Border Remedial Authority: Section 5(a)**

Section 3 of the Act amended the FTC’s core jurisdictional provisions in section 5(a) of the FTC Act to confirm the FTC’s authority to challenge frauds originating abroad that harm U.S. consumers,<sup>66</sup> and frauds involving material conduct in the United States, including those that victimize foreign consumers.<sup>67</sup> The amendment also clarified the availability of monetary restitution as a remedy for domestic and foreign victims of FTC Act violations.<sup>68</sup>

This amendment has greatly enhanced the FTC’s ability to pursue cross-border fraud. Before the passage of the Act, the FTC faced legal challenges to its authority to take action in cross-border matters, particularly in the area of restitution or consumer redress.<sup>69</sup> Since the passage of the Act, the FTC has used the provisions of section 5(a)—in briefs in litigated cases and in negotiations with opposing counsel in a wide range of FTC investigations and cases—to defeat challenges to its jurisdiction and redress authority.

For example, the FTC relied on section 5(a) in *FTC v. Innovative Marketing, Inc.*, discussed above, in which the FTC alleged that the defendants deceptively distributed the “scareware” software to millions of consumers throughout the United States and abroad. The FTC cited the provisions of section 5(a) in two separate briefs—one, opposing the defendants’ attempts to modify the preliminary injunction, the other opposing the defendants’ efforts to avoid contempt of court and repatriation of their foreign assets to the United States. In response to the defendants’ arguments that the FTC did not have jurisdiction because of the foreign aspects of the case, the FTC invoked the “long history of federal case law applying the FTC Act to transnational frauds that harm consumers” and the statutory SAFE WEB amendments, noting that: “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.”<sup>70</sup> The court concluded that the FTC had jurisdiction and rejected the defendants’ arguments.

In *FTC v. Jaivin Karnani*,<sup>71</sup> the FTC obtained a temporary restraining order against U.S. defendants who operated their business from California and allegedly deceptively sold electronics exclusively to British consumers. In so doing, the FTC relied on its authority

to seek redress for foreign consumers under section 5(a) in support of its motion for temporary restraining order to enjoin the defendants' deceptive conduct.<sup>72</sup> The FTC similarly asserted this authority in support of its motion for temporary restraining order in *FTC v. MCS Programs, LLC*,<sup>73</sup> a telemarketing case involving an allegedly fraudulent debt reduction operation that targeted both U.S. and Canadian consumers. The court granted the motion, and the case is still pending.

The FTC has also relied on the amendments to section 5(a) in negotiations with opposing lawyers in a variety of matters, including a matter involving jurisdiction over foreign defendants and several matters concerning the amount of redress related to international sales of certain products. In most cases, the new provisions of section 5(a) have helped the FTC avoid litigation over the issue. In sum, in just a few short years, the amendments have enabled the FTC to dispose of spurious challenges to its jurisdiction quickly.

Moreover, since the passage of the Act, other foreign governments have taken steps to provide agencies with similar authority to obtain remedies for consumers—including those outside their jurisdictions—which would help American consumers who are victims of foreign scams. Since the passage of the Act, the UK government has recommended that Parliament provide this authority to the relevant UK agencies.<sup>74</sup> In addition, the Canadian Parliament approved amendments to the Canadian Competition Act, which took effect on March 12, 2009, to increase penalties for deceptive marketing conduct and to expressly empower the courts to award restitution to victims of false or misleading representations.<sup>75</sup> This authority would apply to foreign victims. Furthermore, in a recent decision, a Canadian appellate court upheld a \$2 million fine under Canada's Competition Act against scam artists based in Toronto even though they exclusively targeted consumers outside of Canada, mostly in the United States.<sup>76</sup>

## V. Legislative Recommendation

Section 14 of the Act directs the FTC to include in its report recommendations for additional legislation. Currently, the Act includes a sunset provision stating that the Act shall expire seven years after the date of enactment. As set forth in this report, the Act has provided the FTC with authority that is essential to combating fraud and deception in the global marketplace, cooperating with foreign partners, and protecting consumers. For example, without the authority provided by the Act, the FTC would not have been able to cooperate meaningfully with foreign authorities to shut down international spam networks or stop deceptive debt collection and advertising practices. In addition, without the Act, the FTC would have been unable to

provide reciprocal investigative assistance to key foreign partners. The FTC's ability to protect consumers in a global economy would be significantly hampered if the Act's authority were to expire.

In addition, as fraudsters increasingly hide behind borders to evade detection and exploit new technologies to deceive consumers around the globe, the need for the authority provided in the Act will only increase. As a result, the FTC will need to rely more heavily on the Act in future years.

Moreover, the sunset provision is a significant obstacle to the conclusion of international agreements that would otherwise lead to enhanced cooperation under the Act. As the FTC negotiates with its foreign partners, these partners want assurances that the FTC will not lose key authority in the future. Foreign partners will be less likely to devote the resources necessary to conclude lasting information agreements if the Act is not permanent. In short, the mere existence of the sunset provision—which would take effect only four years from now in 2013—currently undermines the effectiveness of the Act and inhibits the FTC's ability to use lasting international agreements to protect consumers.

Further, the Act has served as an example for similar efforts in other countries to seek broader authority to share information with foreign agencies.<sup>77</sup> In Canada, government officials have cited the Act in proceedings before Parliament in support of incorporating similar authority in Bill C-27, the Electronic Commerce Protection Act, which would provide the privacy, consumer protection, and telecommunications agencies in Canada the authority to obtain and share evidence with foreign agencies that have reciprocal legislation.<sup>78</sup> In New Zealand, public officials also considered the Act as they developed the recent Privacy (Cross-Border Information) Amendment Bill, which inserts a clause into the New Zealand Privacy Act of 1993 to facilitate cooperation in privacy complaints handling with overseas privacy enforcement authorities.

Indeed, it would be anomalous for the FTC to face the threat of losing authority upon which other countries have relied to enhance their own ability to fight cross-border fraud. Moreover, in circumstances where the foreign country requires the requesting agency to have reciprocal legislation, the FTC would no longer qualify as an agency that is eligible to seek and receive foreign assistance in its investigations if the Act were to expire.

In light of 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, the FTC respectfully requests that Congress repeal the sunset provision now.

Accordingly, the FTC requests that Congress amend the Act as follows:

Section 13 of the U.S. SAFE WEB Act, Pub. L. No. 109-455, 120 Stat. 3372, is hereby repealed.

~~SEC. 13. SUNSET.~~

~~This Act, and the amendments made by this Act, shall cease to have effect on the date that is 7 years after the date of enactment of this Act.~~

## VI. Conclusion

The Act has provided the FTC with authority that is—and will be—vital to its ability to protect U.S. consumers in the global marketplace. Since the passage of the Act, the FTC has used its new information sharing and investigative assistance authority to help bring down international spam gangs, Canadian fraud artists, and several other malefactors injuring both U.S. and foreign consumers. The placement of an FTC attorney at DOJ has facilitated increased participation in the initiation of foreign proceedings seeking evidence or the recovery of assets for FTC cases. The FTC has also used its SAFE WEB authority to develop and strengthen important relationships with foreign partners, including operating a thriving International Fellows Program and initiating negotiations on international consumer protection agreements with key partners. In short, the Act has been essential in the FTC’s investigations and enforcement of consumer protection laws in the global economy. In light of the important role that the Act has played in enhancing the FTC’s ability to carry out its mission, the FTC recommends that Congress repeal the sunset provision. In so doing, Congress would preserve the FTC’s much-needed authority to protect consumers effectively from global threats. The Act has helped the FTC to overcome enforcement challenges it faced in the past, and it is critical to the FTC’s ability to combat threats consumers will face in the future.

## Endnotes

1. 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)).
2. *See infra* Sections IV and V. Section IV outlines the reporting requirements, and Section V outlines the legislative recommendation.
3. *Hearing on Internet Fraud Before the Comm. on Finance*, 107th Cong. (2001) (statement of the Federal Trade Commission, presented by Hugh Stevenson), *available at* [www.ftc.gov/os/2001/04/internetfraudstate.htm](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, presented by Eileen Harrington), *available at* [www.ftc.gov/os/2001/05/internetfraudttmy.htm](http://www.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, presented by Hugh Stevenson) [hereinafter *Cross-Border Fraud Hearing*], *available at* [www.ftc.gov/os/2001/06/cbftest.htm](http://www.ftc.gov/os/2001/06/cbftest.htm).
4. FTC, *Cross-Border Fraud Trends January-December 2002*, at 5 (Feb. 2003). The Consumer Sentinel Network is an investigative cyber tool and complaint database, restricted to law enforcement use, that provides civil and criminal enforcement organizations immediate and secure access to identity theft, Internet, telemarketing (including Do Not Call), and other consumer-related complaints. Because many consumers do not submit complaints after becoming a victim of a scam, the number of cross-border complaints reported to the Consumer Sentinel Network likely understates the scope of the problem.
5. *Cross-Border Fraud Hearing*, *supra* note 3 (testimony of Hugh Stevenson).
6. Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2005, S. 1608, 109th Cong. (2005); *see* S. Rep No. 109-219 (2006). The proposed legislation largely tracked the substantive provisions of an earlier bill—the International Consumer Protection Act of 2004, H.R. 3413, 108th Cong. (2004); S. 1234, 108th Cong. (2004).
7. FTC, *The US SAFE WEB Act: Protecting Consumers From Spam, Spyware, and Fraud*, A Legislative Recommendation to Congress (June 2005) [hereinafter *US SAFE WEB Act Report*], *available at* [www.ftc.gov/reports/ussafeweb/USSAFEWEB.pdf](http://www.ftc.gov/reports/ussafeweb/USSAFEWEB.pdf).
8. OECD, *Guidelines for Protecting Consumers Across Borders from Fraudulent and Deceptive Commercial Practices* (2003), *available at* [www.oecd.org/dataoecd/24/33/2956464.pdf](http://www.oecd.org/dataoecd/24/33/2956464.pdf). The guidelines were developed by the OECD’s Committee on Consumer Policy, under the chairmanship of former FTC Commissioner Mozelle Thompson. The Guidelines set forth a number of approaches countries could use to address cross-border consumer fraud and deception. The OECD Guidelines specifically recommended that member countries “identify obstacles to effective cross-border co-operation in the enforcement of laws designed to protect consumers against fraudulent and deceptive commercial practices,” and consider “adopting or amending national legislation to overcome these barriers.” *Id.*
9. Indeed, Congress had already provided many of the tools that the FTC sought to agencies such as the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC), whose areas of responsibility went “global” long before burgeoning cross-border fraud and deception against consumers brought cross-border cooperation to the forefront of the FTC’s consumer protection efforts. For example, in 1990, Congress expanded the SEC’s powers to gather and share relevant information with its foreign counterparts. *See* Securities Acts Amendments of 1990, Pub. L.

- 101-550, 104 Stat. 2713 (1990). A few years later, it gave the CFTC similar powers and mechanisms to cooperate with foreign authorities. *See* Futures Trading Practices Act of 1992, Pub. L. No. 102-546, § 302, 106 Stat. 3590, 3622 (1992).
10. *See* Statement of Federal Trade Commission Chairman Deborah Platt Majoras on Passage of the US SAFE WEB Act by the 109th Congress, *available at* [www.ftc.gov/speeches/majoras/061211statementUSSafeweb.pdf](http://www.ftc.gov/speeches/majoras/061211statementUSSafeweb.pdf).
  11. *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* [www.ftc.gov/opa/2006/12/safewebLaw.shtm](http://www.ftc.gov/opa/2006/12/safewebLaw.shtm).
  12. *See* 15 U.S.C. §§ 46(f), 57b-2(b)(6).
  13. *See* 15 U.S.C. § 46(j).
  14. *Id.*
  15. 15 U.S.C. § 46(j)(2)(B). *See also* 28 U.S.C. § 1782.
  16. 15 U.S.C. § 57b-2(f)(2)(A)(i)-(ii).
  17. *Id.* at § 57b-2(f)(2)(A)(iii).
  18. *See* 15 U.S.C. § 57b-2(f)(2)(B).
  19. *See* 15 U.S.C. § 57b-2a.
  20. *See* 15 U.S.C. § 57b-2b.
  21. *See* 15 U.S.C. § 45(a)(4).
  22. *See* 15 U.S.C. § 56(c)(1).
  23. *See* 15 U.S.C. § 57c-1.
  24. *See* 15 U.S.C. § 46(j)(4).
  25. Section 14 of the U.S. SAFE WEB Act, Pub. L. No. 109-455, 120 Stat. 3372 (2006).
  26. FTC, Cross-Border Fraud Complaints January-December 2008, at 4 (May 2009). In addition to storing complaints submitted to the FTC, the Consumer Sentinel Network also includes complaints filed with the Internet Crime Complaint Center, Better Business Bureaus, Canada's Phone Busters, the U.S. Postal Inspection Service, and the Identity Theft Assistance Center, among others.
  27. *Id.* at 5. During calendar year 2008, the Consumer Sentinel Network received over 1.2 million consumer complaints. *Id.* at 2. Over 643,000 complaints were fraud-related complaints. *Id.* "A fraud complaint is cross-border if: (1) a U.S. consumer complained about a company located in Canada or another foreign country; (2) a Canadian consumer complained about a company located in the U.S. or another foreign country; or (3) a consumer from a foreign country complained about a company located in the U.S. or Canada. Company location is based on addresses reported by the complaining consumers and, thus, likely understates the number of cross-border complaints." *Id.* at 2.
  28. *Id.* at 3.
  29. *Id.*
  30. *Id.* at 4.
  31. *Id.* at 6.
  32. *Id.* at 11.

33. *Id.*
34. *Id.* at 8.
35. *Id.* at 9.
36. *Id.*
37. *Id.*
38. 15 U.S.C. §§ 46(f), 57b-2(b)(6).
39. 16 C.F.R. § 4.11(j); *see also* Access Requests from Foreign Law Enforcement Agencies for Consumer Protection Materials, 72 Fed. Reg. 28,851 (Fed. Trade Comm'n May 23, 2007) (final rule amendment).
40. *Id.*
41. *Id.*
42. The Act does not authorize the FTC to share information with agencies from countries that the Secretary of State has determined repeatedly support international terrorism. *See* 15 U.S.C. § 57b-2(b)(6)(D). This prohibition also applies to agencies submitting requests for investigative assistance. *See* 15 U.S.C. § 46(j)(7).
43. *See, e.g., FTC v. Atkinson*, No. 08-CV-5666 (N.D. Ill. Filed Oct. 6, 2008), press release *available at* [www.ftc.gov/opa/2008/10/herbalkings.shtm](http://www.ftc.gov/opa/2008/10/herbalkings.shtm); *FTC v. Innovative Mktg., Inc.*, No. RDB 08CV3233 (D. Md. filed Dec. 2, 2008), press release *available at* [www.ftc.gov/opa/2008/winsoftware.shtm](http://www.ftc.gov/opa/2008/winsoftware.shtm); *FTC v. Cash Today, Ltd.*, 3:08-cv-00590-BES-VPC (D. Nev. filed Nov. 6, 2008), press release *available at* [www.ftc.gov/opa/2008/11/cashtoday.shtm](http://www.ftc.gov/opa/2008/11/cashtoday.shtm).
44. *FTC v. MCS Programs, LLC*, No. C095380 RJB (W.D. Wash. filed June 25, 2009), press release *available at* [www.ftc.gov/os/caselist/0823216/index.shtm](http://www.ftc.gov/os/caselist/0823216/index.shtm).
45. *FTC v. B.C. Ltd. 0763496*, No. C07-1755RSM (W.D. Wash. filed Oct. 31, 2007), press release *available at* [www.ftc.gov/opa/2007/11/cashcorner.shtm](http://www.ftc.gov/opa/2007/11/cashcorner.shtm).
46. 15 U.S.C. § 46(j).
47. The FTC has received two other preliminary requests for SAFE WEB investigative assistance from foreign agencies that were ultimately resolved through voluntary cooperation with third parties. In addition, the FTC is currently considering whether to provide investigative assistance pursuant to the Act in response to two other requests from foreign agencies.
48. 15 U.S.C. § 46(j)(2)(B); *see also* 28 U.S.C. § 1782.
49. *See* 15 U.S.C. § 46(j)(4). The provision authorizes the Commission to enter into binding international agreements with a foreign law enforcement agency if the agency has a legal basis for requiring execution of such an agreement in order to provide reciprocal assistance or to provide materials or information to the Commission.
50. *See* 1 U.S.C. § 112a-112b; 22 C.F.R. § 181.1 *et seq.*
51. Relevant Canadian and European Union laws envision a formal international agreement for certain types of enforcement cooperation. *See* Competition Act [Canada], Part III: Mutual Legal Assistance, § 30 *et seq.*, *available at* [www.competitionbureau.gc.ca/internet/index.cfm?itemID=1304&lg=e](http://www.competitionbureau.gc.ca/internet/index.cfm?itemID=1304&lg=e); *see also* European Commission Regulation 2006/2004/EC, 2004 J.O. (L 364) 1, *available at* [http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l364/l\\_36420041209en00010011.pdf](http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l364/l_36420041209en00010011.pdf).
52. 15 U.S.C. § 57b-2a.



53. 15 U.S.C. § 57b-2a(g).
54. 15 U.S.C. § 57b-2b.
55. During a hearing on September 17, 2003, before the House Energy & Commerce Subcommittee on Commerce, Trade, and Consumer Protection, one of the corporate witnesses testified as follows regarding the need for immunity when providing information voluntarily to the FTC:

Mr. MacCarthy. I don't have much to add on the civil versus criminal part of your question, but if I could take the opportunity to quickly respond to Marc's point about immunity. It puts companies like ours in a very awkward situation if we receive a request for information from the government, and it is all perfectly legitimate and above-board, and we cooperate with that. And in a later process it sounds that somebody somewhere and not us, but somebody somewhere else didn't follow all the rules and regulations. If then we are liable for violating other rules, it makes it very, very difficult for us to be cooperative in that kind of circumstance. So for us the immunity provision does create an enormously important part of the legislation.

*The International Consumer Protection Act of 2003: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Prot. of the H. Comm. on Energy and Commerce, 108th Cong. 49-50 (2003).*

56. 15 U.S.C. § 57b-2b(b).
57. 15 U.S.C. § 57b-2b(a), (d)(2)-(3).
58. 15 U.S.C. § 57b-2b(c), (d)(4).
59. Section 14(8) of U.S. SAFE WEB Act.
60. 15 U.S.C. § 56(c)(1).
61. This provision recognizes that attorneys who are specially appointed by the Attorney General have the same authority to conduct legal proceedings as United States attorneys.
62. *See FTC v. Data Bus. Solutions, Inc.*, No. 08-CV-2783 (N.D. Ill. filed May 14, 2008), press release available at [www.ftc.gov/opa/2008/06/ils.shtm](http://www.ftc.gov/opa/2008/06/ils.shtm).
63. *See* 15 U.S.C. § 57c-1. Congress also authorized the FTC to detail its own officers or employees temporarily to foreign government agencies. *Id.* However, the Act states that staff arrangements under this provision need not be reciprocal. The FTC has used this outbound staff exchange authority four times: to send a staff attorney from the Office of International Affairs to the UK Office of Fair Trading twice; to send a merger attorney from the Bureau of Competition to the European Commission's Directorate General for Competition; and to send an economist from the Bureau of Economics to the UK Competition Commission. The latter two outbound details were part of reciprocal staff exchanges.
64. Fellows and interns came from Argentina, Australia, Austria, Brazil, Canada, Egypt, the European Commission, Israel, Mexico, Poland, Singapore, Switzerland, and Turkey.
65. Fellows have also made significant contributions to the FTC's competition work. For example, fellows from Singapore and Brazil assisted in merger investigations, including conducting analyses of data to evaluate the likely competitive effects of the proposed transactions.
66. 15 U.S.C. 45(a)(4)(A)(i).
67. 15 U.S.C. 45(a)(4)(A)(ii).
68. 15 U.S.C. 45(a)(4)(B).

69. See US SAFE WEB Act Report, *supra* note 7, at 14-15.
70. 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).
71. *FTC v. Jaivin Karnani*, No. CV09-5276 DDP (C.D. Cal. filed July 20, 2009), press release available at [www.ftc.gov/os/caselist/0923081/index.shtm](http://www.ftc.gov/os/caselist/0923081/index.shtm). In this case, the FTC obtained a temporary restraining order against a California company that allegedly misled consumers in the United Kingdom about the applicability of UK product warranties and their ability to cancel orders or obtain refunds. The FTC alleged that the U.S. company also misrepresented to UK consumers that it participated in the U.S.-EU Safe Harbor program. This program enables companies to self-certify that the personal information they collect from EU consumers is being treated in accordance with requirements based on the EU data protection law. Many UK consumers submitted complaints about the U.S. company through [econsumer.gov](http://econsumer.gov), a website sponsored by the International Consumer Protection Enforcement Network (ICPEN) that collects cross-border complaints. Such complaints are available to ICPEN member agencies. They are also available through the FTC's Consumer Sentinel Network and can be accessed by the FTC and other network members throughout the U.S., Canada, and Australia.
72. Plaintiff's Memorandum in Support of Noticed Motion for Temporary Restraining Order and Other Equitable Relief and Motion for Show Cause Hearing, *FTC v. Jaivin Karnani*, No. CV09-5276 DDP (C.D. Cal. filed July 20, 2009).
73. *FTC v. MCS Programs, LLC*, No. C095380 RJB (W.D. Wash. filed June 25, 2009), press release available at [www.ftc.gov/os/caselist/0823216/index.shtm](http://www.ftc.gov/os/caselist/0823216/index.shtm).
74. United Kingdom Department for Business, Innovation and Skills, A Better Deal for Consumers, Delivering Real Help Now and Change for the Future, at 54 (July 2009), available at [www.berr.gov.uk/files/file52072.pdf](http://www.berr.gov.uk/files/file52072.pdf).
75. See [www.cb-bc.gc.ca/eic/site/cb-bc.nsf/eng/h\\_03036.html](http://www.cb-bc.gc.ca/eic/site/cb-bc.nsf/eng/h_03036.html).
76. *R. v. Stucky*, No. CA C46382, 2009 CarswellOnt 745 (Ont. Feb. 17, 2009) (Westlaw). See [www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03117.html](http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03117.html).
77. See, e.g., Letter from Jennifer Stoddart, Privacy Commissioner of Canada, to Hugh Stevenson, Deputy Director for Consumer Protection of the Office of International Affairs, Federal Trade Commission (June 13, 2008); Letter from Jennifer Stoddart, Privacy Commissioner of Canada, to Jon Leibowitz, Chairman, Federal Trade Commission (Aug. 28, 2009).
78. 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 [www.crtc.gc.ca/eng/NEWS/SPEECHES/2009/s090618.htm](http://www.crtc.gc.ca/eng/NEWS/SPEECHES/2009/s090618.htm) (advocating for an amendment that would give the CRTC power to obtain and share information with authorities in foreign countries, such as the United States, that have reciprocal legislation).

# Appendix A

## U.S. SAFE WEB Act Requests Resulting in Enforcement Actions or Ongoing Investigations

## U.S. SAFE WEB Act Requests Resulting in Enforcement Actions or Ongoing Investigations

No.	Foreign Agencies Requesting Information Sharing or Investigative Assistance	Resulting proceedings
1.	Royal Canadian Mounted Police	The FTC obtained a \$1 million default judgment. Consumer Protection BC (British Columbia) filed concurrent proceedings in Canada. Canadian authorities arrested one of the suspects, who subsequently fled to a third country after being released on bail. Law enforcement authorities continue to pursue this matter.
2.	(1) Competition Bureau Canada (2) Australian Communications & Media Authority	The FTC obtained a \$3.7 million default judgment against five defendants and a \$29,000 settlement with the remaining defendants.
3.	Toronto Police Service (multiple requests for same matter)	The FTC obtained an \$18 million consent agreement. Canadian authorities arrested individuals associated with the scam and took action to shut down fraudulent operations in several locations.
4.	(1) New Zealand Department of Internal Affairs (2) Australian Communications & Media Authority	The FTC and the New Zealand Department of Internal Affairs filed enforcement actions against individuals associated with this operation. The FTC obtained a \$15.15 million default judgment against the principal defendant and his company, and a \$3.77 million default judgment against the remaining three corporate defendants. In addition, the FTC obtained a settlement agreement with the remaining individual defendant. The New Zealand Department of Internal Affairs obtained three settlements totaling NZ\$250,000 (approximately US\$179,000). The FBI executed search warrants, and one of the suspects named in the FTC action pled guilty to a federal criminal charge.

<b>No.</b>	<b>Foreign Agencies Requesting Information Sharing or Investigative Assistance</b>	<b>Resulting proceedings</b>
5.	Competition Bureau Canada	The FTC, with the assistance of the Competition Bureau Canada, brought an enforcement action, which is still pending. The FTC also used its attorney on detail at DOJ's Office of Foreign Litigation to facilitate the filing of an application seeking to compel evidence in a Canadian court for use in the domestic proceedings.
6.	(1) City of London Police (2) UK Office of Fair Trading	The FTC obtained a \$1 million settlement agreement with the U.S. and UK defendants.
7.	Royal Canadian Mounted Police (multiple requests for same matter)	Canadian authorities froze the targets' assets in Canada. The Royal Canadian Mounted Police arrested two suspects who await extradition.
8.	(1) Competition Bureau Canada (2) Ontario Provincial Police (3) Royal Canadian Mounted Police	The FTC launched Operation Tele-PHONEY, which included 13 actions filed by the FTC, including at least two cross-border actions, and 180 cases total brought by various authorities in the U.S. and Canada. The actions brought by Competition Bureau Canada resulted in criminal charges against four defendants and the conviction of two previously-charged defendants, one of whom pled guilty.
9.	(1) Competition Bureau Canada (2) Security Service of Ukraine (3) Ministry of the Attorney General (Ontario, Canada)	The FTC, with assistance from the Competition Bureau, brought an enforcement action. The FTC obtained entries of default against two defendants and settlements with two defendants, requiring them to forfeit over \$100,000. The case is still pending with respect to the remaining defendants.
10.	Office of the Privacy Commissioner of Canada	The Office of the Privacy Commissioner relied substantially on information provided by the FTC in issuing its findings that the company had violated Canadian law.
11.	Australian Communications & Media Authority (CIDs issued on behalf of ACMA)	ACMA monitored the target's conduct and obtained its voluntary compliance with Do Not Call regulations.

<b>No.</b>	<b>Foreign Agencies Requesting Information Sharing or Investigative Assistance</b>	<b>Resulting proceedings</b>
12.	OPTA (Dutch Independent Post and Telecommunications Authority) (CID issued on behalf of OPTA)	OPTA used the information provided by the FTC to confirm a suspect's identity and involvement in the operation and continues to investigate the matter.
13.	Competition Bureau Canada	The FTC filed an enforcement action, and the matter is still pending. The Canadian authorities executed a search warrant concurrent with the filing of the FTC action, and their criminal investigation is ongoing.
14.	Competition Bureau Canada	The FTC filed an enforcement action, and the matter is still pending. Canadian authorities executed a search warrant on the defendants' business premises in Canada, and their investigation is ongoing.
15.	Royal Canadian Mounted Police	The Royal Canadian Mounted Police used this information to facilitate an enforcement sweep. In a related matter, the FTC obtained an \$18 million consent agreement.
16.	Toronto Police Service (CID issued on behalf of the Toronto Police Service)	The Toronto Police Service arrested 13 individuals associated with the scam, one of whom was directly linked to the scam as a result of the information the FTC provided. This case involved a substantial number of U.S. victims.
17.	Competition Bureau Canada (CIDs issued on behalf of the Competition Bureau)	The Canadian authorities executed a search warrant. The FTC previously brought an enforcement action against the individuals involved in this scam.
18.	Canadian Radio-television and Telecommunications Commission (CRTC)	The FTC brought an enforcement action, and the matter is still pending.
19.	Toronto Police Service (CIDs issued on behalf of the Toronto Police Service)	The Toronto Police Service is prosecuting the suspect. The information the FTC provided helped the Toronto Police Service identify U.S. victims of the scam.

# Appendix B

## FTC Enforcement Actions With Public Cross-Border Components

## FTC Enforcement Actions With Public Cross-Border Components

(Cases filed between January 2007 and October 2009)<sup>1</sup>

No.	Case Caption	Conduct Alleged	Cross-Border Component(s)	Initial Press Release
<b>2009 Cases</b>				
1.	<i>FTC v. MoneyGram Int'l</i> , No. 1:09-cv-06576 (N.D. Ill. filed Oct. 19, 2009).	Defendants allegedly allowed their money transfer system to be used by fraudulent telemarketers to bilk consumers out of tens of millions of dollars.	Canadian agents allegedly used MoneyGram outlets in Canada to defraud U.S. consumers.	<a href="http://www.ftc.gov/opa/2009/10/moneygram.shtm">www.ftc.gov/opa/2009/10/moneygram.shtm</a>
2.	<i>FTC v. Jaivin Karnani, et al.</i> , No. 09-CV-5276 (C.D. Cal. filed July 20, 2009).	The FTC alleged that defendants deceptively advertised and sold consumer electronic products, such as cameras, video game systems, and computer software, via the Internet to consumers in the United Kingdom.	The case exclusively targeted consumers in the United Kingdom. UK authorities assisted the FTC with this investigation. Many consumers in the United Kingdom registered complaints with the FTC by using the website <a href="http://www.econsumer.gov">www.econsumer.gov</a> .	<a href="http://www.ftc.gov/opa/2009/08/bestpriced.shtm">www.ftc.gov/opa/2009/08/bestpriced.shtm</a>

<sup>1</sup> The list of cross-border cases includes cases filed in which public information indicates that one or more of the defendants is located abroad and/or there is some other significant foreign component, such as a large number of foreign victims, efforts to recover substantial foreign assets, or substantial investigative assistance by a foreign law enforcement authority. It does not attempt to capture every case involving foreign victims, foreign evidence, or foreign assets; many cases have some such connection, but this information is not always publicly disclosed.



No.	Case Caption	Conduct Alleged	Cross-Border Component(s)	Initial Press Release
3.	<i>FTC v. Diamond Phone Card, Inc., et al.</i> , No. 09-CV-3257 (E.D.N.Y. filed July 29, 2009).	Defendants allegedly misrepresented the number of calling minutes consumers could obtain using prepaid calling cards created and/or distributed by defendants, and failed to disclose, or disclose adequately, fees that had the effect of reducing the number of calling minutes available to consumers using prepaid calling cards created and/or distributed by defendants.	The consumer protection agencies in El Salvador, Colombia, Egypt, Mexico, Panama, and Peru assisted the FTC with this investigation.	<a href="http://www.ftc.gov/opa/2009/08/diamond.shtm">www.ftc.gov/opa/2009/08/diamond.shtm</a>
4.	<i>FTC v. Paul Navestad, et al.</i> , No.09CV6329T (W.D.N.Y. filed June 25, 2009).	Defendants allegedly waged an automated robocall campaign promoting bogus claims that consumers were qualified for grant money from the government, private foundations, and wealthy individuals.	The defendants conducted business through companies that were purportedly based abroad.	<a href="http://www.ftc.gov/opa/2009/07/shortchange.shtm">www.ftc.gov/opa/2009/07/shortchange.shtm</a>
5.	<i>FTC v. MCS Programs, LLC, et al.</i> , No. 09-CV-5380 (W.D. Wa. filed June 25, 2009).	Defendants allegedly used telemarketing robocalls and the Internet to sell a phony “Rapid Debt Reduction” program to consumers in the United States and Canada.	The case included foreign victims. Canadian authorities provided assistance in this matter.	<a href="http://www.ftc.gov/opa/2009/07/shortchange.shtm">www.ftc.gov/opa/2009/07/shortchange.shtm</a>

No.	Case Caption	Conduct Alleged	Cross-Border Component(s)	Initial Press Release
6.	<i>FTC v. In Deep Servs., Inc.</i> , No. 09-CV-01193 (C.D. Cal. filed June 23, 2009).	Defendants allegedly deceived consumers by promising them free government grant money to use for personal expenses or to pay off debt. The defendants allegedly failed to disclose adequately that consumers would be enrolled in a membership program that cost as much as \$94.89 a month.	Defendant used an offshore payment processor.	www.ftc.gov/opa/2009/07/shortchange.shtml
7.	<i>FTC v. Wagner Ramos Borges</i> , No. 09-CV-1634 (D. Md. filed June 22, 2009).	The defendant allegedly operated a bogus employment scam.	The defendant is allegedly located abroad.	www.ftc.gov/opa/2009/07/shortchange.shtml
8.	<i>FTC v. 6654916 Canada Inc., a Canadian Corporation, d/b/a National Yellow Pages Online Inc., et al.</i> , No. 09C 3159 (N.D. Ill. filed May 27, 2009).	The FTC alleged that defendants deceptively marketed directory listings to businesses and other organizations in the United States.	The Canadian Competition Bureau and Project COLT, a multi-agency, U.S.-Canada partnership formed in the 1990s to combat telemarketing fraud, provided assistance with this investigation. The defendants were based in Canada.	www.ftc.gov/opa/2009/06/optmirage.shtml

No.	Case Caption	Conduct Alleged	Cross-Border Component(s)	Initial Press Release
9.	<i>FTC v. Integration Media Inc., a corporation, d/b/a GoAm Media, et al.</i> , No. 09C 3160 (N.D. Ill. filed May 27, 2009).	The FTC alleged that defendants deceptively marketed directory listings to businesses and other organizations in the United States.	The Canadian Competition Bureau and Project COLT, a multi-agency, U.S.-Canada partnership formed in the 1990s to combat telemarketing fraud, provided assistance with this investigation. The defendants were based in Canada.	www.ftc.gov/opa/2009/06/optmirage.shtm
10.	<i>FTC v. 6253547 Canada, Inc., et al.</i> , No. 1:09CV01211 (N.D. Ill. filed May 27, 2009) (consolidated with <i>FTC v. Integration Media, Inc.</i> after initial filing).	The FTC alleged that defendants deceptively marketed directory listings to businesses and other organizations in the United States.	The Canadian Competition Bureau and Project COLT, a multi-agency, U.S.-Canada partnership formed in the 1990s to combat telemarketing fraud, provided assistance with this investigation. The defendants were based in Canada.	www.ftc.gov/opa/2009/06/optmirage.shtm
11.	<i>FTC v. 6555381 Canada, Inc., a corporation, d/b/a Reed Publishing, et al.</i> , No. 09C 3158, (N.D. Ill. filed May 27, 2009).	The FTC alleged that defendants deceptively marketed directory listings to businesses and other organizations in the United States.	The Canadian Competition Bureau and Project COLT, a multi-agency, U.S.-Canada partnership formed in the 1990s to combat telemarketing fraud, provided assistance with this investigation. The defendants were based in Canada.	www.ftc.gov/opa/2009/06/optmirage.shtm

No.	Case Caption	Conduct Alleged	Cross-Border Component(s)	Initial Press Release
12.	<i>FTC v. Sean Cantkier, et al.</i> , No. 09-CV-00894 (D.D.C. May 14, 2009).	The defendants allegedly diverted consumers who searched online for the free government mortgage loan assistance program to commercial websites that offer loan modification services for a fee.	One of the defendants was located in Malaysia.	www.ftc.gov/os/caselist/0923147/index.shtm
13.	<i>FTC v. Romeo, et al.</i> , No. 2:09-cv-01262-WJM-CCC (D.N.J. filed Mar. 20, 2009).	The defendants allegedly made false and deceptive claims when advertising purported hoodia products to trade customers.	The defendants sold products in the United States and other countries.	www.ftc.gov/opa/2009/04/nutraceuticals.shtm
<b>2008 cases</b>				
14.	<i>FTC v. Innovative Mktg., Inc., et al.</i> , Civil Action No.: RDB 08CV3233 (D. Md. filed Dec. 2, 2008).	Defendants allegedly misrepresented that they conducted scans of consumers' computers and falsely indicated that the scans detected a variety of security or privacy issues.	The case included British and Canadian defendants. One of the companies was incorporated in Belize and maintained offices in the Ukraine.	www.ftc.gov/opa/2008/12/winsoftware.shtm
15.	<i>FTC and the State of Nevada v. Cash Today, Ltd., et al.</i> , No. 3:08-cv-00590-BES-VPC (D. Nev. filed Nov. 6, 2008).	Defendants allegedly violated the FTC Act, Truth in Lending Act, and Regulation Z by not disclosing key loan terms to U.S. consumers and using abusive and deceptive debt collection tactics.	Some of the defendants were based in the United Kingdom. The UK's Office of Fair Trading assisted the FTC with this investigation.	www.ftc.gov/opa/2008/11/cashtoday.shtm

No.	Case Caption	Conduct Alleged	Cross-Border Component(s)	Initial Press Release
16.	<i>FTC v. CyberSpy Software, LLC, et al.</i> , No. 08-cv-08172 (M.D. Fla. filed Nov. 5, 2008).	Defendants allegedly sold keylogging spyware to clients who may have used it to secretly monitor unsuspecting consumers' computers.	Some clients reported purchasing the software from people online who they now suspect are foreign scam artists.	www.ftc.gov/opa/2008/11/cyberspy.shtml
17.	<i>FTC v. 9163-7710 Québec, Inc., et al.</i> , No. 3:08-CV-02131-GAG (D.P.R. filed Oct. 28, 2008).	Defendants allegedly violated the FTC Act by misrepresenting that they had preexisting relationships with consumers, that consumers had agreed to purchase defendants' services, and that consumers owed money for defendants' services.	This case was brought with the assistance of the Royal Canadian Mounted Police and Project COLT, a multi-agency, U.S.-Canada initiative formed in the 1990s to combat telemarketing fraud.	www.ftc.gov/opa/2008/10/yellowpages.shtml
18.	<i>FTC v. RCA Credit Servs., LLC, et al.</i> , No. 8:08-CV-2062-T-27MAP (M.D. Fla. Oct. 16, 2008).	Defendants allegedly operated a deceptive credit repair scheme and failed to comply with requirements of the Credit Repair Organizations Act.	Some of the defendants were located in the Philippines.	www.ftc.gov/opa/2008/10/opcleansweep.shtml
19.	<i>FTC v. Atkinson, et al.</i> , No. 08-CV-5666 (N.D. Ill. filed Oct. 9, 2008).	Defendants violated the FTC Act and CAN-SPAM Act by deceptively marketing a variety of products through spam messages, including a male-enhancement pill, prescription drugs, and a weight-loss pill.	Defendants operated in Australia, New Zealand, Cyprus, and the United States. The New Zealand Department of Internal Affairs and the Australian Communications and Media Authority provided assistance with this investigation.	www.ftc.gov/opa/2008/10/herbalkings.shtml

No.	Case Caption	Conduct Alleged	Cross-Border Component(s)	Initial Press Release
20.	<i>FTC v. Nur-Gen Nutrition, Inc., et al.</i> , No. 1:08-cv-05309 (N.D. III filed Sept. 18, 2008).	Defendants allegedly deceptively advertised bogus cancer remedies.	Defendants sold cancer remedies to victims in foreign countries.	www.ftc.gov/opa/2008/09/boguscures.shtml
21.	<i>FTC v. Advanced Patch Techs., Inc., et al.</i> , No. 1:04-CV-0670 (N.D. Ga. Modified settlement filed Sept. 16, 2008). (Original consent agreement was obtained in March 2004.)	Defendants allegedly violated a 2004 FTC consent order by continuing to make false claims about their weight-loss product.	Defendants made deceptive claims in brochures accompanying product shipments intended for sale to overseas consumers.	www.ftc.gov/opa/2008/09/patchnr.shtml
22.	<i>FTC v. 9107-4021 Québec, Inc., a corporation, also d/b/a Med Provisions, et al.</i> , No. 1:08-cv-01051-DCN (N.D. Ohio filed Aug. 12, 2008).	Defendants allegedly violated the FTC Act and the Telemarketing Sales Rule by making misrepresentations to U.S. consumers about an online pharmacy and their Medicare benefits.	Defendants were based in Montreal, Canada. Canada's Competition Bureau provided substantial investigative assistance in this case.	www.ftc.gov/opa/2008/05/telephoney.shtml

<b>No.</b>	<b>Case Caption</b>	<b>Conduct Alleged</b>	<b>Cross-Border Component(s)</b>	<b>Initial Press Release</b>
23.	<i>FTC v. 6554962 Canada Inc., d/b/a Union Consumer Benefits, et al.</i> No. 1:08-cv-02309 (N.D. Ill. filed Apr. 23, 2008).	Defendants violated the FTC Act and the Telemarketing Sales Rule by telemarketing worthless medical discount packages to elderly consumers throughout the United States. Defendants also violated the law by calling many consumers on the Do Not Call Registry.	Defendants were based in Canada. Canada's Competition Bureau assisted with this investigation.	<a href="http://www.ftc.gov/opa/2008/05/telephone.shtm">www.ftc.gov/opa/2008/05/telephone.shtm</a>
24.	<i>FTC v. NHS Sys., Inc., et al.</i> , No. 08-cv-2215 (E.D. Pa. filed May 13, 2008).	Defendants allegedly engaged in deceptive telemarketing and unauthorized billing practices. They purported to contact consumers on behalf of government agencies and charged consumers to enroll in programs without their consent.	Key defendants were based in Canada and St. Lucia. Canadian authorities assisted with serving process on some of the defendants located in Canada.	<a href="http://www.ftc.gov/os/caselist/0823117/index.shtm">www.ftc.gov/os/caselist/0823117/index.shtm</a>
25.	<i>FTC v. Datacom Mktg., Inc., et al.</i> , No. 06 C 2574 (N.D. Ill. filed May 6, 2008).	Defendants ran a cross-border fraud operation scamming American businesses into paying for business directories and listings they did not order.	Canada's Competition Bureau, the Service de Police de la Ville de Montreal, and the Toronto Strategic Partnership assisted with this investigation.	<a href="http://www.ftc.gov/opa/2008/05/datacom.shtm">www.ftc.gov/opa/2008/05/datacom.shtm</a>

<b>No.</b>	<b>Case Caption</b>	<b>Conduct Alleged</b>	<b>Cross-Border Component(s)</b>	<b>Initial Press Release</b>
26.	<i>FTC v. Data Bus. Solutions Inc., et al.</i> , No. 08-CV-2783 (ND. Ill. filed May 14, 2008).	Defendants allegedly ran a cross-border fraud operation scamming American businesses and non-profit organizations by sending them fake invoices disguised to look like annual bills from their existing domain name registrars for their websites.	Competition Bureau Canada, the Toronto Police Service – Fraud Squad, the Ontario Ministry of Government Services, the Ontario Provincial Police – Anti-Rackets, the Royal Canadian Mounted Police, and the United Kingdom’s Office of Fair Trading assisted with this investigation. The FTC’s attorney on detail at DOJ’s Office of Foreign Litigation worked with foreign counsel to file an application seeking to compel evidence in a Canadian court that could be used in the domestic proceeding.	<a href="http://www.ftc.gov/opa/2008/06/ils.shtm">www.ftc.gov/opa/2008/06/ils.shtm</a>
27.	<i>FTC v. Alternatel, Inc., et al.</i> , No. 1:08-cv-21433-AJ (S.D. Fla. filed May 19, 2008).	Defendants allegedly violated the FTC Act by misrepresenting the number of calling card minutes consumers could use to contact people in foreign countries, failing to disclose that consumers’ cards would be charged whether or not the calls went through, and charging hidden fees.	The consumer protection agencies in Colombia, Egypt, El Salvador, Mexico, Panama, and Peru provided assistance in this investigation.	<a href="http://www.ftc.gov/opa/2008/06/alternatel.shtm">www.ftc.gov/opa/2008/06/alternatel.shtm</a>



No.	Case Caption	Conduct Alleged	Cross-Border Component(s)	Initial Press Release
28.	<i>FTC v. 1522838 Ontario Inc., a corporation, d/b/a International Industrial Trade Directory, et al.</i> , No.: 06C-5378 (N.D. III filed Apr. 15, 2008).	The defendants, a Kenyan citizen, American citizen, and Canadian citizen, all of whom were residents of Canada, violated the FTC Act by misleading consumers into believing they owed money for advertising and other products and services that were not ordered or delivered.	The Toronto Strategic Partnership provided assistance with this investigation.	<a href="http://www.ftc.gov/opa/2008/04/industrialtrade.shtml">www.ftc.gov/opa/2008/04/industrialtrade.shtml</a>
29.	<i>FTC v. Oleg Oks, et al.</i> , No. 1:05-cv-05389 (N.D. III. filed Mar. 18, 2008).	Defendants engaged in deceptive telemarketing practices by falsely promising delivery of credit cards and free gifts and debiting consumers' bank accounts.	The Toronto Strategic Partnership and United Kingdom's Office of Fair Trading provided assistance with this investigation.	<a href="http://www.ftc.gov/opa/2008/05/pacliberty.shtml">www.ftc.gov/opa/2008/05/pacliberty.shtml</a>
30.	<i>FTC v. Clifton Telecard Alliance One LLC, et al.</i> , No.: 2:08-cv-1480-pgs-es (D.N.J. filed Apr. 2, 2008).	Defendants allegedly violated the FTC Act by misrepresenting the number of calling card minutes consumers could use to contact people in foreign countries, failing to disclose that consumers' cards would be charged whether or not the calls went through, and charging hidden fees.	The consumer protection agencies in Colombia, Egypt, El Salvador, Mexico, Panama, and Peru provided assistance with this investigation.	<a href="http://www.ftc.gov/opa/2008/03/cta.shtml">www.ftc.gov/opa/2008/03/cta.shtml</a>

No.	Case Caption	Conduct Alleged	Cross-Border Component(s)	Initial Press Release
<b>2007 cases</b>				
31.	<i>FTC, State of Illinois, State of Iowa, State of Nevada, State of North Carolina, State of North Dakota, State of Ohio, and State of Vermont v. Your Money Access, LLC, et al.</i> , No.:07-547 (E.D. Pa. filed Dec. 6, 2007).	Defendants, including a payment processing company, allegedly violated federal and state laws by debiting, or attempting to debit, money from consumers' bank accounts on behalf of numerous fraudulent telemarketers and Internet-based merchants.	Defendants' clients included foreign entities such as Canadian telemarketers.	www.ftc.gov/opa/2007/12/yma.shtm
32.	<i>FTC v. B.C. Ltd.</i> 0763496, <i>d.b.a. Cash Corner Services, Inc., et al.</i> , No. C07-1755 (W.D. Wa. filed Nov. 19, 2007).	Defendants violated the FTC Act and the Telemarketing Sales Rule by running a bogus lottery and prize promotion scam that provided consumers with counterfeit cashier's checks and false promises of large prizes.	Defendants were based in Canada.	www.ftc.gov/opa/2007/11/cashcorner.shtm
33.	<i>FTC v. Spear Sys., Inc., et al.</i> , No. 07C-5597 (N.D. Ill. filed Oct. 3, 2007).	Defendants violated the FTC Act and the CAN-SPAM Act by sending deceptive e-mail messages about hoodia weight-loss products and human growth hormone anti-aging products and making claims about those products that were false and unsubstantiated.	Defendants were based in Australia and Canada.	www.ftc.gov/opa/2007/10/hoodia.shtm

<b>No.</b>	<b>Case Caption</b>	<b>Conduct Alleged</b>	<b>Cross-Border Component(s)</b>	<b>Initial Press Release</b>
34.	<i>FTC v. Practical Mktg., Inc., et al.</i> , No. 3:07-cv-00685-JPG-DGW (S.D. Ill. filed Sept. 28, 2007).	Defendants allegedly violated the FTC Act and the Telemarketing Sales Rule by assisting telemarketers who were purchasing lists in order to solicit U.S. consumers to pay advance fees to get “guaranteed” credit cards with substantial credit limits. The lists included consumers’ credit card and bank account information, exposing thousands of consumers to possible identity theft, and violating federal law.	Defendants sold lists to Canadian telemarketers.	<a href="http://www.ftc.gov/opa/2007/10/listbrokers.shtml">www.ftc.gov/opa/2007/10/listbrokers.shtml</a>
35.	<i>FTC v. Silit Nutraceuticals, LLC, et al.</i> , No. 07C 4541 (N.D. Ill. filed Aug. 13, 2007).	Defendants violated the FTC Act and the CAN SPAM Act by sending deceptive e-mail messages about hoodia weight-loss products and human growth hormone anti-aging products and making claims about those products that were false and unsubstantiated.	Defendants’ companies were based in the Caribbean.	<a href="http://www.ftc.gov/opa/2007/08/hoodia.shtml">www.ftc.gov/opa/2007/08/hoodia.shtml</a>
36.	<i>FTC v. 9131-4740 Québec, Inc., a corporation, also d/b/a Fusion Telekom, et al.</i> , No. 07-cv-02242 (N.D. Ohio filed Jul. 25, 2007).	Defendants allegedly violated the Telemarketing Sales Rule and the FTC Act by deceptively marketing telephone calling cards.	Defendants were based in Canada.	<a href="http://www.ftc.gov/opa/2007/07/fusion.shtml">www.ftc.gov/opa/2007/07/fusion.shtml</a>

No.	Case Caption	Conduct Alleged	Cross-Border Component(s)	Initial Press Release
37.	<i>FTC v. Crystal Ewing, David Ewing, Consumer Direct Enterprises, Top Choice, Classic Productions, and Response Processing</i> , FTC No. 062-3025 (D. Nev. filed Apr. 11, 2007).	Defendants allegedly ran a deceptive prize promotion scheme.	Defendants targeted consumers in the United States, Canada, and the United Kingdom.	www.ftc.gov/opa/2007/04/consumerdirect.shtm
38.	<i>FTC v. Mystery Shop Link, LLC, et al.</i> , No. CV07-01791 SJO (Shx) (C.D. Cal. filed Mar. 16, 2007).	Defendants allegedly deceptively marketed a mystery shopper job program to consumers.	Defendants targeted consumers in the United States and Canada. One of the defendants was located in Australia.	www.ftc.gov/opa/2007/03/mysteryshop.shtm
39.	<i>FTC v. Select Personnel Mgmt., Inc., et al.</i> , No. 07C 0529 (N.D. Ill. filed Jan. 29, 2007).	Defendants engaged in fraudulent telemarketing to consumers throughout the United States, falsely claiming they could reduce consumers' credit card interest rates.	Defendants were based in Canada.	www.ftc.gov/opa/2007/02/sms.shtm
40.	<i>FTC v. Lane Labs-USA, Inc., et al.</i> , No. 00CV3174 (D.N.J. contempt action filed Jan. 12, 2007).	Defendants allegedly violated a 2000 FTC order prohibiting deceptive advertising claims and requiring reliable and scientific evidence to substantiate advertising claims.	The FTC deposed an expert witness in Canada.	www.ftc.gov/opa/2007/01/lanelabs.shtm

<b>No.</b>	<b>Case Caption</b>	<b>Conduct Alleged</b>	<b>Cross-Border Component(s)</b>	<b>Initial Press Release</b>
41.	<i>FTC v. International Prod. Design, Inc., et al.</i> , No. 1:97-CV-01114-AVB (E.D. Va. contempt action filed Jan. 8, 2007).	Defendants allegedly violated a 1998 order prohibiting them from deceptively marketing invention promotion services.	One of the original corporate defendants was based in the United Kingdom.	www.ftc.gov/opa/2007/03/ipd.shtm

Federal Trade Commission  
1-1877-FTC-HELP  
[ftc.gov](http://ftc.gov)