The U.S. SAFE WEB Act and the FTC's Fight Against Cross-Border Fraud

A Report to Congress

October 20, 2023

FEDERAL TRADE COMMISSION

Lina M. Khan, Chair
Rebecca Kelly Slaughter, Commissioner
Alvaro M. Bedoya, Commissioner

Contents

The Federal Trade Commission ("FTC" or "Commission") submits this report to update Congress on implementation of the U.S. SAFE WEB Act of 2006, as required by the 2020 law that extended the Act until September 30, 2027.[1] As directed by Congress, this report describes the FTC's use of and experience with the Act, including the number of cross-border complaints received, the foreign agencies with which the FTC has cooperated, foreign FTC litigation, and legislative recommendations based on that experience. This report supplements the FTC's 2009 report to Congress on the FTC's first three years of experience in implementing the Act.[2]

Executive Summary

In 2006, recognizing the increasing threats facing consumers in the global marketplace, Congress passed the Undertaking Spam, Spyware, And Fraud Enforcement with Enforcers beyond Borders Act of 2006: the U.S. SAFE WEB Act ("SAFE WEB").[3] Since then, SAFE WEB has become an indispensable tool helping the FTC to combat cross-border fraud, and to otherwise protect consumers in an increasingly global and digital economy. **It is critical that the FTC have these tools to continue fighting such fraud and other misconduct, which continues to cost American consumers billions of dollars.**

SAFE WEB expressly affirms the FTC's authority to pursue deceptive or unfair acts or practices involving foreign actors targeting Americans, as well as U.S. business conduct affecting foreign consumers. It also provides the FTC with enhanced law enforcement tools essential to effective cross-border enforcement and cooperation, including in the areas of (1) information sharing, (2) investigative assistance, (3) jurisdictional authority, (4) confidentiality, and (5) enforcement relationships.

Since SAFE WEB's passage, the FTC has used the Act to:

- Share confidential and compelled information from FTC files in **175** instances with **43** law enforcement agencies in **20** different countries.
- Provide investigatory assistance by issuing more than **140** civil investigative demands ("CIDs") in **67** investigations on behalf of **21** foreign agencies from **eight** countries.
- Pursue cross-border enforcement matters facilitated by information sharing and cooperation with foreign law enforcement agencies.
- Engage in **148** staff exchanges to build cooperation with foreign counterparts, in particular bringing colleagues from more than **41** foreign jurisdictions to work with FTC attorneys, economists, investigators, and more, and sending FTC staff on **15** short-term secondments.

---

[1] Pub. L. No. 116-173, 134 Stat. 837 (2020), available at https://www.congress.gov/116/plaws/publ173/PLAW-116publ173.pdf.
[2] The U.S. SAFE WEB Act: The First Three Years. A Report to Congress (Dec. 2009) ("2009 SAFE WEB Report"), https://www.ftc.gov/reports/us-safe-web-act-first-three-years-federal-trade-commission-report-congress.
[3] 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)), available at http://uscode.house.gov/statutes/pl/109/455.pdf.

With SAFE WEB, the FTC has pursued and stopped harmful conduct in the U.S. and successfully defended against challenges to its jurisdictional authority over foreign companies targeting American consumers. The FTC has also worked with numerous foreign enforcers to stop cross-border injury and frauds. For example, SAFE WEB enabled the FTC to:

- Shut down a real estate investment scam (known as "Sanctuary Belize") that took in more than $100 million, the largest such scheme the FTC has ever targeted.
- Cooperate with privacy authorities in Canada and the United Kingdom ("U.K.") to pursue actions against AshleyMadison.com, an online dating site that deceived consumers and failed to protect the account and profile information of more than 36 million individuals.
- Work with foreign law enforcement agencies to stop fraudulent money transfers to Western Union and MoneyGram locations in Spain in connection with a Nigerian email scam.

SAFE WEB has been instrumental in the FTC's fight against cross-border fraud, which continues to plague consumers and shows no sign of abating. Since the FTC first began tracking cross-border fraud complaints in 1996, the FTC has received over **2.6 million** consumer reports of cross-border fraud. In the preceding eight and half years from January 1, 2015, to June 30, 2023, alone, consumers reported:

- Over **1.4 million** incidents of cross-border fraud.
- More than **$5.2 billion** in losses.

During those same eight and a half years, American consumers in particular reported:

- Nearly **half a million** incidents of cross border fraud.
- **$2.49 billion** in losses to cross-border fraud.

These figures, already staggering, almost certainly understate the true amount of cross-border fraud that consumers face. Only a small percentage of consumers who encounter fraud file complaints, and the cross-border aspects of many frauds are not always apparent to the consumers themselves.

SAFE WEB has also become a key part of international enforcement arrangements to protect privacy in connection with the international data transfers that are an increasingly common part of the consumer marketplace.[4] The FTC plays an enforcement role in protecting the transfer of personal data from

[4] *See*, *e.g.*, U.S. Department of Commerce, Data Privacy Framework Program, EU-U.S. Data Privacy Framework Principles, https://www.dataprivacyframework.gov/s/framework-text (last accessed Sept. 28, 2023); *See also* Section II.B. (discussing *CafePress*).

numerous foreign countries. These data transfers in turn support trillions of dollars in cross-border commercial transactions.[5]

Given the magnitude of the cross-border issues and the important role that SAFE WEB plays in the FTC's response, we recommend permanent reauthorization of the Act. Allowing SAFE WEB to lapse would deprive the FTC of its most important tool to fight cross-border fraud and put at risk the FTC's cross-border enforcement efforts.

[5] *See* White House, Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework (Mar. 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

Introduction

Cross-border fraud remains a serious and persistent problem in the United States. Since 1999, the FTC has received over **1.3 million reports** of cross-border fraud from U.S. consumers.

The U.S. SAFE WEB Act serves as a vital tool in the FTC's arsenal to fight cross-border fraud and protect consumers from unfair and deceptive acts and practices. SAFE WEB expressly affirms the FTC's authority to pursue foreign conduct that causes reasonably foreseeable injury to American consumers, or that involves material conduct here in the United States.[6] SAFE WEB also promotes global partnerships and enforcement cooperation with foreign counterparts. The Act provides a framework to engage in cross-border assistance, including information sharing[7] and investigative support.[8] Further, the Act encourages broader cross-border cooperation with law enforcement agencies around the world through agreements, memoranda of understanding ("MOUs"),[9] and staff exchanges.[10] The record of activities since our last report to Congress in 2009[11] shows that SAFE WEB has met Congress's objective to provide more effective cross-border consumer protection enforcement.

The FTC has been tracking and combatting cross-border fraud for nearly three decades. During that time the nature and origins of cross-border fraud have evolved, and cross-border fraud continues to cause significant harm to consumers. In 1996, the earliest year for which the FTC has cross-border fraud data, less than 1% of fraud reported to the FTC was cross-border.[12] Nearly 30 years later, in 2022, the most recent full year for which the FTC has complaint data, over **11%** of all fraud reported to the FTC was cross-border, with consumers reporting fraud originating in **225 countries**. Since 2006, the year Congress passed the U.S. SAFE WEB Act, U.S. consumers alone have reported over **1.14 million** instances of cross-border fraud and **more than $4.4 billion in financial losses**.

The important tools Congress provided to the FTC through SAFE WEB have enabled the FTC to better protect consumers from cross-border fraud. In the 16 years since Congress passed SAFE WEB, the FTC has used the Act's powers to assist or share information with foreign law enforcement in over **300** instances. The FTC has also brought at least 145 enforcement actions with a cross-border element.

---

[6] Section 3 of the SAFE WEB Act codified at Section 5(a) of the FTC Act, 15 U.S.C. §45(a)(4)(A) (providing that "unfair and deceptive acts and practices" includes those that "(i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States.")
[7] Sections 4(a) and 6(a) of the SAFE WEB Act codified at Sections 6(f) and 21(b)(6) of the FTC Act, 15 U.S.C. §46(f) and 57b-2(b)(6).
[8] Section 4(b) of the SAFE WEB Act codified at Section 6(j) of the FTC Act, 15 U.S.C. §46(j).
[9] FTC MOUs and other cooperation arrangements, including international agreements, are available at FTC, Legal Library: Cooperation Agreements, https://www.ftc.gov/legal-library/browse/cooperation-agreements (last accessed Sept. 28, 2023).
[10] Section 9 of the SAFE WEB Act codified at Section 25A of the FTC Act, 15 U.S.C. § 57c-1 (authorizing the FTC "to retain or employ officers or employees of foreign government agencies on a temporary basis as employees of the Commission").
[11] 2009 SAFE WEB Report, https://www.ftc.gov/reports/us-safe-web-act-first-three-years-federal-trade-commission-report-congress).
[12] *Id*. at 2 (reporting a total of 1,128 complaints).

These enforcement actions have been supported, either directly or indirectly, by SAFE WEB's promotion of cross-border engagement with foreign partners.

Report Overview

In this report, the FTC provides data on cross-border fraud and its use of the authority Congress granted to the Commission through SAFE WEB. This report, provided more than a decade after the FTC first reported to Congress on SAFE WEB, reflects the FTC's ongoing analysis of cross-border fraud, and its further experience with the tools provided under the Act. The report is organized as follows:

Section I of the report discusses the multi-billion-dollar scourge of cross-border fraud and its impact on consumers, as shown in particular through analysis of cross-border complaint data. Appendix A provides further details on international fraud complaint data. Appendix B provides further details about (a) the Consumer Sentinel Network – the FTC's system for collecting and sharing consumer complaints; (b) FTC actions to expand the system's data contributors and enforcement users; and (c) the FTC's public reporting of international complaint trends through its Tableau Public webpages.[13]

Section II of the report discusses how Congress and the FTC have responded to this challenge. Section II.A. describes some of the FTC's early efforts to combat cross-border fraud and how those efforts led to the FTC recommending, and Congress passing, the U.S. SAFE WEB Act. It also describes the key enforcement tools Congress granted to the FTC through SAFE WEB.

Section II.B. highlights the FTC's cross-border enforcement activities since SAFE WEB's passage. These actions demonstrate the importance of SAFE WEB's express affirmation of the FTC's authority to pursue deceptive or unfair acts or practices involving foreign commerce. Appendix C provides a list of FTC enforcement actions with public cross-border components since Congress passed the Act. The cases listed cover a broad range of subjects, ranging from fraud, spam, and spyware to deceptive advertising, data security, and privacy.

Section II.C. details how the FTC regularly uses SAFE WEB to increase cross-border enforcement cooperation to help protect consumers from cross-border fraud and other misconduct. It explains FTC efforts to share information with and assist foreign law enforcement, highlighting notable enforcement examples. It also explains how the FTC has relied on SAFE WEB to grow and deepen our relationships with foreign law enforcement agencies and various international networks, including through MOUs and staff exchanges.

---

[13] Consumer Sentinel has a five-year data retention policy, with reports older than five years purged biannually. When the FTC drafted this report, it maintained Sentinel data for January 1, 2019, to June 30, 2023 (published July 25, 2023). This report relies on that data, historical reports, and limited archived data currently retained by the FTC, including for the period January 1, 2015, to December 31, 2018. Certain current Sentinel data that the FTC makes public on a quarterly basis is available at https://public.tableau.com/app/profile/federal.trade.commission/viz/federal.trade.commission#!/. Certain historical Sentinel reports are available at https://www.ftc.gov/enforcement/consumer-sentinel-network/reports.

Section III of the report provides the FTC's legislative recommendation. The FTC again urges Congress to make SAFE WEB permanent by removing the sunset provision currently set to expire on September 30, 2027, thereby preserving the Commission's jurisdiction over foreign commerce and its ability to effectively cooperate with foreign law enforcement. As shown in this report, the U.S. SAFE WEB Act and its tools have been essential to the FTC's efforts to combat cross-border fraud and other consumer harms. Without these tools, the FTC's ability to cooperate and share information with foreign law enforcement agencies would be severely curtailed, putting at risk the Commission's ability to stop unfair or deceptive acts or practices involving foreign commerce. The FTC also urges Congress to amend Section 13(b) of the FTC Act to restore the FTC's ability to provide refunds to harmed consumers and prevent bad actors from keeping money generated by breaking the law.

I. Cross-Border Fraud

Consumer complaints collected by the FTC demonstrate that cross-border fraud is significant and persistent.[14] Since 1996, when the FTC first began tracking cross-border complaints, the FTC has received over **2.6 million** reports of cross-border fraud,[15] including over **1.4 million** since January 1, 2015. American consumers alone have reported over **1.3 million** incidents of cross-border fraud since 1999 (the earliest that data specific to U.S. consumers is available to the FTC), including **1.14 million** since 2006 (when Congress passed SAFE WEB) and 482,600--**nearly half a million**--since January 1, 2015.[16]

While significant on its own, cross-border fraud also accounts for a notable portion of the total fraud that consumers face. Since the FTC's 2009 SAFE WEB Report (from January 1, 2009, to June 30, 2023), **nearly 10%** of all fraud reports received by the FTC were cross-border, including 12.5% and 11.4% of

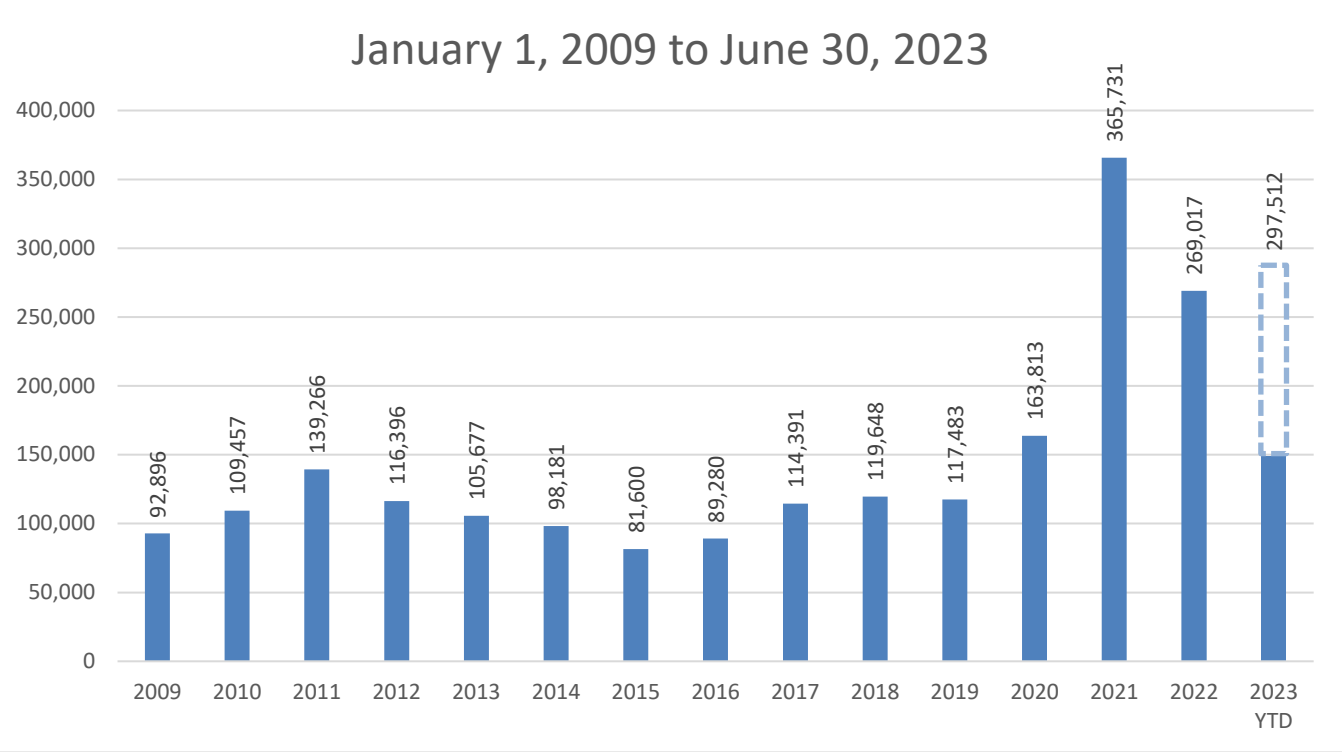
[14] The FTC considers a complaint to be "cross-border" when the consumer country is provided, the company country is provided, and those countries are different. Prior to 2013, the FTC considered a complaint to be cross-border if: (1) a U.S. consumer complained about a company located in a country other than the U.S., (2) a Canadian consumer complained about a company located in a country other than Canada, or (3) a consumer located in a country other than the U.S. or Canada complained about a company located in the U.S. or Canada. This excluded a small number of complaints where both the consumer and company location were in countries other than the U.S. or Canada.

[15] The FTC received 542,885 cross-border fraud complaints from January 1, 1996, to December 31, 2008. (*See* 2009 SAFE WEB Report at 5.) Between January 1, 2009, and June 30, 2023, the FTC received an additional 2,131,592 cross-border fraud complaints. (*See Figure 1*).

[16] U.S. consumers filed 500,251 cross-border fraud reports between January 1, 1999, and December 31, 2009. *See* Prepared Statement of the Federal Trade Commission on Reauthorizing the U.S. SAFE WEB Act of 2006 before the Subcommittee on Commerce, Manufacturing, and Trade of the Committee on Energy and Commerce, United States House of Representatives by Hugh Stevenson, Deputy Director, Office of International Affairs (July 12, 2012) ("July 2012 Prepared Statement of Hugh Stevenson") at 3, https://www.ftc.gov/legal-library/browse/prepared-statement-federal-trade-commission-reauthorizing-us-safe-web-act-2006. U.S. consumers filed 381,260 reports between January 1, 2010, and December 31, 2014. S*ee* FTC, Consumer Sentinel Network, International Consumer Complaints, January – December 2014 (June 2015) at 7, https://www.ftc.gov/system/files/documents/reports/international-consumer-complaints-cy-2014/cy-2014_international.pdf (providing data on fraud complaints by U.S. consumers against foreign businesses for calendar years 2010 to 2014). Between January 1, 2015, and June 30, 2023, U.S. consumers reported the following number of cross-border fraud complaints: 51,408 (2015); 56,923 (2016); 52,829 (2017); 50,800 (2018); 45,194 (2019); 69,184 (2020); 73,894 (2021); 56,117 (2022); 26,251 (through June 30, 2023).

complaints filed in 2021 and 2022, respectively.[17] In addition, in 2021 and 2022, roughly **one in five** of the fraud reports that reported both a consumer and a business location were cross border.[18] The number of cross-border fraud complaints the FTC received each year since 2009, plus partial year data for 2023, appears in *Figure 1*.[19]

Figure 1: Cross Border Complaint Count

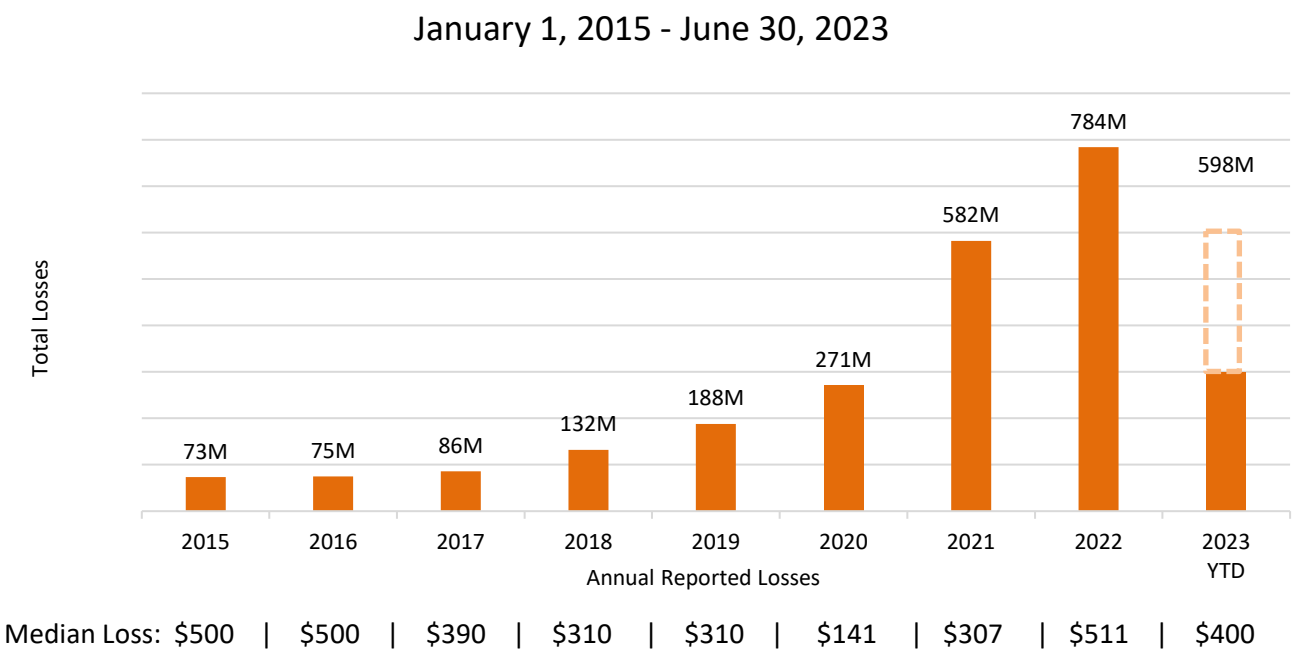


Cross-border fraud results in significant financial harm to consumers. Since 2006, U.S. consumers have reported over **$4.4 billion dollars** in losses to cross border fraud.[20] This includes **$2.49 billion** since

[17] Between January 1, 2009, and June 30, 2023, the FTC received 22,309,302 fraud complaints. In 2021 and 2022, the FTC received 2,923,241 and 2,369,527 fraud complaints, respectively. *See Figure 1* for cross-border fraud data.
[18] If consumers do not report their location or the location of the business, the FTC cannot accurately categorize their reports as cross-border or non-cross-border. In 2021 and 2022, it was "unknown" whether 38% and 39% of consumer reports, respectively, were cross-border or non-cross border.
[19] The increase in cross-border fraud reports in 2021 reflects, in part, a significant number of new reports from a recently added data contributor located outside of the U.S. Additionally, the increase in cross-border fraud reports in 2021 and subsequent decrease in 2022 is consistent with all fraud complaints and is likely related, in part, to the COVID-19 global pandemic.
[20] U.S. consumers reported $1.4 billion in losses to cross-border fraud between January 1, 2006, and December 31, 2011. *See* July 2012 Prepared Statement of Hugh Stevenson at 3. U.S. consumers reported $578 million in losses from January 1, 2012, to December 31, 2014. S*ee* Consumer Sentinel Network, International Consumer Complaints, January – December 2014

January 1, 2015.[21] In addition, when reporting about cross-border fraud, most U.S. consumers (between 62% and 76% each year from 2015 to 2022) have reported a financial loss,[22] with annual median reported losses ranging from $141 to $511. Total annual and median reported losses by U.S. consumers to cross-border fraud for the years 2015 to 2022 are set forth in *Figure* 2. U.S. consumers also reported an additional $299.4 million in losses to cross-border fraud during the first half of 2023 – more than the total annual losses reported by U.S. consumers to cross-border fraud each year between 2015 and 2020.

Figure 2: Reported U.S. Consumer Loss to Cross-Border Fraud



These figures, while staggering, almost certainly understate the true extent of cross-border fraud. This is because consumers report only a small percentage of scams to government agencies or other organizations, such as the Better Business Bureaus ("BBBs"), that contribute data to the FTC's

(FTC, June 2015) at 9 (providing data on amount paid by U.S. consumers against foreign companies for calendar years 2012 to 2014), https://www.ftc.gov/enforcement/consumer-sentinel-network/reports. Since January 1, 2015, U.S. consumers have reported $2.49 billion in losses to cross-border fraud. S*ee Figure 2*.

[21] For this same period, all consumers (both U.S. and foreign) have reported the following annual losses to cross-border fraud, which totals over $5.2 billion: $137.8M (2015); $141.8M (2016); $168.6M (2017); $243.2M (2018); $406.3M (2019); $619.9M (2020); $1.289B (2021); $1.557B (2022); $693.9M (through June 30, 2023).

[22] Since January 1, 2015, the following percentage of U.S. consumers have reported a financial loss when reporting about cross-border fraud: 70% (2015); 71% (2016); 62% (2017); 67% (2018); 63% (2019); 76% (2020); 70% (2021); 65% (2022).

Consumer Sentinel system.[23] In addition, when reporting fraud, consumers may not even know that a foreign entity is involved.[24] Foreign scammers often mislead consumers about or conceal their locations, including by using phone numbers that appear to be from the U.S.,[25] VoIP technology such as spoofing (*i.e.*, transmitting fake caller ID information),[26] fake social media profiles,[27] and other tactics. Companies with a foreign connection may also conceal a connection with an additional foreign country or with the United States. The FTC's enforcement action against *Best Priced Brands* (*see* Section II.B., *infra*) illustrates how simple tactics can easily confuse consumers as to a company's location.

U.S. consumers also continue to encounter fraud from businesses operating from jurisdictions around the world.[28] Since 2019, consumers have reported fraud connected with **231 different** countries. The top 10 countries identified by U.S. consumers in connection with their fraud complaints for the period between January 1, 2019, and June 30, 2023, combined (during which this detailed data is currently available) is set forth in *Figure 3*. This includes China,[29] Canada, the U.K., India, and Mexico, which

---

[23] *See, e.g.,* Keith B. Anderson, To Whom Do Victims of Mass-Market Consumer Fraud Complain? (May 24, 2021), https://ssrn.com/abstract=3852323 or http://dx.doi.org/10.2139/ssrn.3852323 (finding that, based on data from surveys of mass-market consumer fraud sponsored by the FTC in 2005, 2011, and 2017, in about 45% of instances, victims complained to someone beyond their family or friends, most frequently to someone directly involved in the transaction, such as the seller or manufacturer, a bank, or credit card company, but only 4.8% of victims complained to a BBB or government agency); *See also, e.g.,* Morgan, Rachel E., U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, Financial Fraud in the United States, 2017, Bulletin NCJ255817 (April 2021), https://bjs.ojp.gov/content/pub/pdf/ffus17.pdf (finding that about 14% of victims of financial fraud reported the fraud to the police, about 12% reported to state or local consumer agencies, such as a state attorney general's office or the BBB, and 10% reported to a federal consumer agency such as the FTC); U.S. Attorney's Office, W.D. Wash., Financial Fraud Crime Victims (Feb. 10, 2015), https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud (estimating that only 15% of fraud victims report their crimes to law enforcement); and U.K. National Crime Agency, https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime (last accessed Sept. 15, 2023) (estimating that 86% of fraud instances in England and Wales go unreported).

[24] For example, between 18% and 39% of fraud complaints received by the FTC between 2019 and 2022 could not be identified as either cross-border or non-cross border. *See also supra* note 19.

[25] *See*, *e.g.*, Colleen Tressler, "One-ring" cell phone scam can ding your wallet, FTC (Feb. 10, 2024), https://consumer.ftc.gov/consumer-alerts/2014/02/one-ring-cell-phone-scam-can-ding-your-wallet (alerting consumers that scammers are using auto-dialers to call consumers from international phone numbers, often in the Caribbean, that appear to come from the U.S.). *See also, e.g.*, AARP, Scammers Lurk Behind Area Code 876 (Sept. 17, 2012), https://www.aarp.org/money/scams-fraud/info-09-2012/beware-area-code-876-nh1788.html.

[26] *See* Federal Communications Commission, Caller ID Spoofing, https://www.fcc.gov/spoofing (last accessed Sept. 15, 2023) ("when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity"). S*ee also*, *e.g.*, *FTC v. Alcazar Networks Inc.*, No. 6:20-cv-2200 (M.D. Ga. Dec. 3 2020), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923259-alcazar-networks-inc (alleging that the defendants facilitated tens of millions of illegal telemarketing phone calls, including some calls from overseas and some that displayed spoofed caller ID numbers; How To Avoid Phone Scams: Don't Trust Caller ID Infographic, FTC (June 2023), https://consumer.ftc.gov/articles/how-avoid-phone-scams-dont-trust-caller-id-infographic.

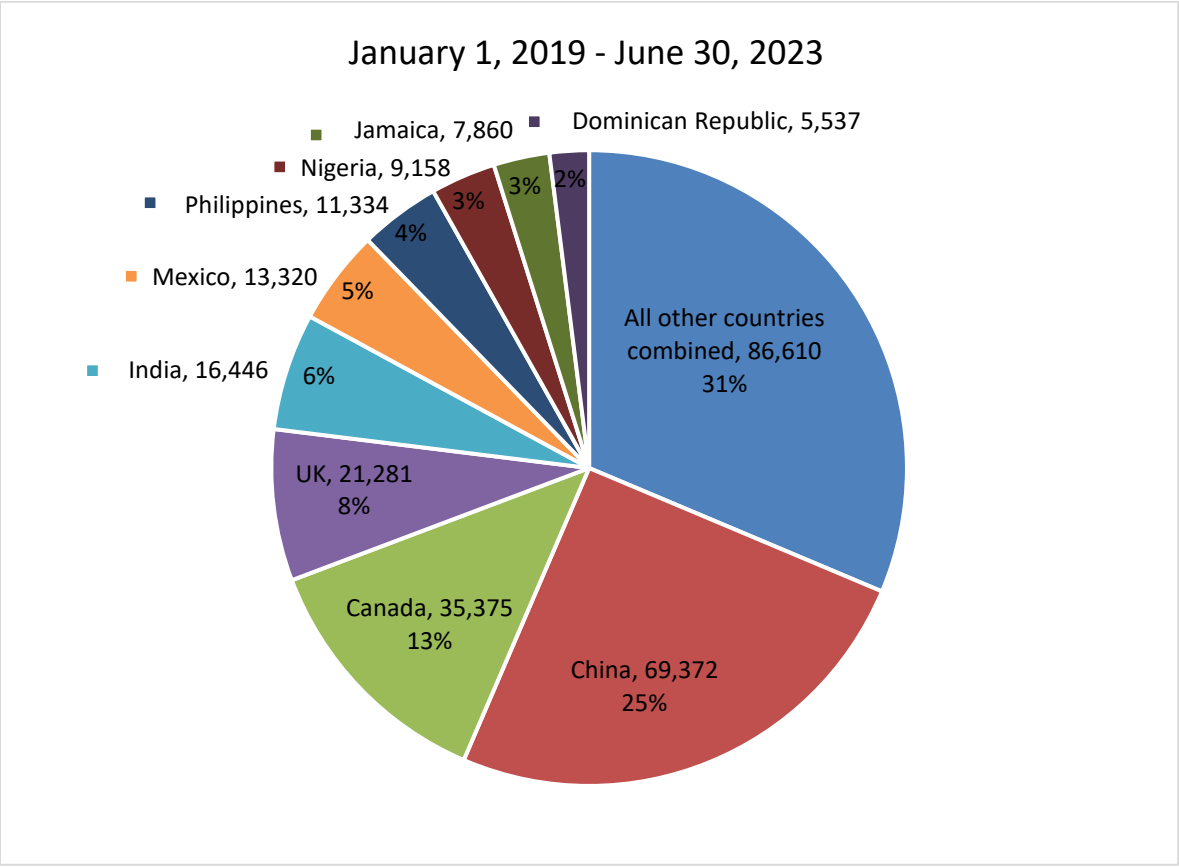
[27] *See*, *e.g.*, FTC, What to Know About Romance Scams (Aug. 2022), https://consumer.ftc.gov/articles/what-know-about-romance-scams (reporting that romance scammers create fake profiles on social media sites); *see also*, *e.g.*, Emma Fletcher, Data Spotlight: Reports of romance scams hit record highs in 2021, FTC (Feb. 2022), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/02/reports-romance-scams-hit-record-highs-2021.

[28] In 2009 the FTC reported that consumer complaints in Sentinel identified companies with connections to over 200 countries. (2009 SAFE WEB Report at 5).

[29] In this report, data for China includes Hong Kong and Macau, which are tracked separately in Sentinel.

combined accounted for more than 55% of cross-border fraud reported by U.S. consumers during this period.

Figure 3: Top 10 Countries for Cross-Border Fraud as Reported by U.S. Consumers



As detailed in Appendix A, recent cross-border fraud reports also show that cross-border problems are multifaceted, with the issues that U.S. consumers are most likely to encounter varying by the foreign country involved. In addition, international fraud reports[30] show that consumers are contacted by and transfer funds to scammers outside of the U.S. in a number of different ways, with the frequency of payment methods also varying by country.

For example, U.S. consumers have reported that two of the most prevalent problems between January 1, 2019, and June 30, 2023, were those related to online shopping (e.g., undisclosed costs, failure to deliver

[30] A fraud complaint is considered to be international when the consumer country or the company country is reported as not the U.S., regardless of any other information.

on time, non-delivery, etc.) and romance scams.[31] U.S. consumers have also reported the following in recent years:

- Online shopping scams frequently originate in China or Canada.
- They often face online shopping and miscellaneous investment frauds (such as virtual currencies and investment advice and seminars) involving entities in the U.K.
- Imposter scams, such as tech support, business imposter, and romance scams, often are connected to India and the Philippines.
- When consumers face fraud from Mexico, it's often friend and family imposter scams.

Recent international fraud reports also show that the means through which scammers contact and obtain funds from consumers has continued to evolve. For example, such reports show:

- Consumers have increasingly been targeted through social media platforms.[32] Increased contact through social media platforms is especially prevalent for fraud originating in China, the U.K., and Mexico, less so for fraud originating in India and Canada.
- Wire transfers continue to be a common method of payment for cross-border fraud. This is often true for fraud originating in Canada and Mexico, but less so for fraud originating in China (excluding Hong Kong and Macau), where most consumers (over 70%) report paying fraudsters through credit or debit cards. Similarly, consumers also regularly report paying scammers in India using payment apps and paying scammers in the U.K. and Hong Kong using cryptocurrency.

And cross-border fraud doesn't just harm American consumers. As some recent enforcement actions demonstrate, entities operating from the U.S. also injure consumers abroad. (*See* Section II.B. discussing *Best Priced Brands* and *Fashion Nova*.) In fact, since 2019, over 61% of all cross-border complaints received by the FTC (a total of 674,133 complaints) were filed by foreign consumers about U.S. entities.

[31] Consumer Sentinel Network report definitions are available at FTC, Consumer Sentinel Network, https://www.ftc.gov/system/files/attachments/data-sets/category_definitions.pdf (last accessed Sept. 28, 2023) and FTC, Consumer Sentinel Network Subcategory Definitions (May 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/CSNPSCFullDescriptions.pdf.

[32] *See* Emma Fletcher, Data Spotlight: Social media a gold mine for scammers in 2021, FTC (Jan. 25, 2022), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021; Press Release, FTC, FTC Issues Orders to Social Media and Video Streaming Platforms Regarding Efforts to Address Surge in Advertising for Fraudulent Products and Scams (Mar. 16, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-issues-orders-social-media-video-streaming-platforms-regarding-efforts-address-surge-advertising.

Such data highlights that cross-border fraud is nuanced and constantly evolving.[33] While the FTC does not act on individual complaints, the complaint data collectively has been critical to identifying problems to address and supports the development of critical evidence in many cases.

II. Responding to the Scourge of Cross-Border Fraud

The FTC has responded forcefully to the problem of cross-border fraud and has worked on a range of issues affecting consumers in the increasingly global consumer marketplace.

A. Early FTC Responses to Cross-Border Fraud

Having observed key developments in technology and global trade and recognizing the possibilities for consumer harm, the FTC began taking early and concrete steps starting in the 1990s to protect consumers from cross-border fraud. Thus in 1992, the FTC helped to found what is now known as the International Consumer Protection and Enforcement Network ("ICPEN") – a network of consumer authorities from various countries dedicated to strengthening cooperation on consumer protection enforcement.[34] The FTC also began building cooperative partnerships with its Canadian counterparts. These efforts resulted in the United States entering into an agreement with Canada on deceptive marketing practices – the FTC's first foreign agreement addressing consumer protection.[35] The FTC also participated in a joint U.S.-Canada working group that prepared a 1997 report on cross-border telemarketing fraud, which recommended that regional task forces be established to maximize cooperation on cross-border fraud, and that governments and agencies examine their laws with an eye toward expanding shared access to cross-border information systems.[36] Consistent with that report, the FTC began building relationships with Canadian federal and provincial authorities through regional

[33] *See also, e.g.*, Office of the United Nations High Commissioner for Human Rights, Online Scam Operations and Trafficking in Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response (2023), https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf (discussing online scam operations and their link to human trafficking in Southeast Asia).

[34] Information on ICPEN, including its members, is available at ICPEN, About, https://icpen.org/who-we-are (last accessed Sept. 28, 2023).

[35] Agreement Between the Government of the United States of America and the Government of Canada Regarding the Application of their Competition and Deceptive Marketing Practices Laws (Aug. 3, 1995), reprinted at 4 Trade Reg. Rep. (CCH) ¶ 13,503, available at https://www.ftc.gov/system/files/attachments/international-competition-consumer-protection-cooperation-agreements/agree_canada.pdf.

[36] Report of the Canada - United States Working Group on Telemarketing Fraud, https://www.justice.gc.ca/eng/rp-pr/other-autre/tf/index.html (last accessed Sept. 28, 2023); *See also* Press Release, U.S. Department of Justice, U.S. and Canada Label Telemarketing Fraud Serious Economic Crime and Propose Recommendations to Fight Growing Problem (Nov. 20, 1997), https://www.justice.gov/archive/opa/pr/1997/November97/491crm.htm.html#:~:text=The%20report%20states%20that%20telemarketing,or%20to%20misrepresent%20the%20true.

partnerships and task forces, such as the Toronto Strategic Partnership[37] and Project COLT.[38] In 1997, the FTC also launched Consumer Sentinel – the first bi-national (U.S. and Canada), multi-state consumer fraud database to track consumer complaints in multiple jurisdictions.[39] In 2001, the FTC then joined with other consumer authorities to launch econsumer.gov – an ICPEN project now available in nine languages – where consumers could report international scams online and learn about other steps to combat fraud.

By the early 2000s, these and other FTC efforts had yielded important enforcement results. By 2001, when the FTC testified before the U.S. Senate, Committee on Governmental Affairs, Subcommittee on Investigations on cross-border fraud, the FTC had already brought multiple cross-border actions, including against sweepstake, advance-fee loan, and foreign lottery telemarketing scams emanating from Canada.[40] This included the FTC's first action against a foreign telemarketing operation for violating the Telemarketing Sales Rule (16 C.F.R. Part 310).[41] And, by the mid-2000s, the FTC had extended its participation in Canada regional partnerships and reached various other agreements and MOUs concerning consumer protection, including with agencies in Australia, Ireland, Mexico, and Spain.[42] Sentinel had also expanded to share econsumer.gov complaint data with other foreign enforcement agencies.[43]

Despite these initiatives, barriers to cross-border enforcement remained, and the FTC identified challenges that needed to be addressed for the agency to keep pace with this growing and evolving problem. Key among these challenges was improving information sharing and increasing the FTC's cooperation with foreign counterparts, further developing Consumer Sentinel, and exploring how the existing legal frameworks for sharing information might be modified to facilitate cooperation in cross-

---

[37] The Toronto Strategic Partnership was formed in February 2000 by the Toronto Police Service, the Ontario Ministry of Consumer and Commercial Relations (now the Ministry of Public and Business Service Delivery), the Competition Bureau of Canada, the U.S. Postal Inspection Service, and the FTC. *See* FTC, Accomplishments of the Toronto Strategic Partnerships 2000 – 2007 (Jan. 2008), https://www.ftc.gov/reports/report-accomplishments-toronto-strategic-partnership-between-united-states-canada-2000-2007.

[38] The Centre of Operations Linked to Telemarketing Fraud ("Project COLT") was launched in 1998 to combat telemarketing-related crime. Members include the FTC, Royal Canadian Mounted Police, Sureté du Québec, Service de Police de la Ville de Montréal, Canada Border Services Agency, the Competition Bureau of Canada, Canada Post, U.S. Homeland Security (U.S. Immigration and Customs Enforcement and the U.S. Secret Service), the U.S. Postal Inspection Service, and the Federal Bureau of Investigation. The current incarnation of Project COLT is known as the Québec Strategic Partnership.

[39] *See* Appendix B for a further discussion of the FTC's efforts to expand Sentinel and consumer complaint reporting.

[40] *See* Prepared Statement of the Federal Trade Commission on "Cross-Border Fraud" before the Subcommittee on Investigations of the Committee on Governmental Affairs, U.S. Senate, Washington, D.C. (June 15, 2001), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-cross-border-fraud/cbftest.pdf.

[41] *See* Press Release, FTC, Arizona Loan Broker, Defendant in FTC Case Against Canadian Loan Scheme, Settles Charges (Apr. 17, 1997), https://www.ftc.gov/news-events/news/press-releases/1997/04/arizona-loan-broker-defendant-ftc-case-against-canadian-loan-scheme-settles-charges.

[42] *See* FTC, International Cooperation Agreements. https://www.ftc.gov/policy/international/international-cooperation-agreements (last accessed Sept. 28, 2023).

[43] A list of current Sentinel members is available at FTC, Consumer Sentinel Network Members, https://www.ftc.gov/enforcement/consumer-sentinel-network/members (last accessed Sept. 28, 2023).

border cases. Thus in 2005 the FTC submitted a report to Congress that proposed amendments to the FTC Act (15 U.S.C. §§ 41, *et seq*.).[44]

In December 2006, to provide more timely and effective international consumer protection, Congress passed the U.S. SAFE WEB Act.[45] Through the Act, Congress provided the FTC with enhanced law enforcement tools, including in the areas of (1) information sharing, (2) investigative assistance, (3) jurisdictional authority, (4) confidentiality, and (5) enforcement relationships. As detailed in this report, these tools have allowed the FTC to better combat cross-border fraud, and to otherwise protect consumers from misconduct in an increasingly global and digital economy. Notably, the U.S. SAFE WEB Act authorizes the FTC to:

- Share compelled and confidential information with foreign law enforcement agencies in appropriate consumer protection matters.[46]
- Provide investigative assistance in consumer protection matters to foreign law enforcement agencies.[47]
- Protect certain material obtained from foreign sources against public disclosure.[48]

Importantly, the Act also confirms that the FTC Act's prohibition against "unfair or deceptive acts or practices" includes certain acts or practices involving "foreign commerce"[49] and supports other international cooperation, including through MOUs and staff exchanges.[50]

Since 2006, Congress has twice extended the SAFE WEB Act, in 2012 and 2020, and the FTC has reported on the Act's use and effectiveness. The FTC submitted a report to Congress on the first three years of SAFE WEB in December 2009.[51] In October 2011, all five FTC Commissioners urged Congress to remove the seven-year sunset provision.[52] In June 2012, the FTC testified in support of

---

[44] The U.S. SAFE WEB Act: Protecting Consumers from Spam, Spyware, and Fraud, A Legislative Recommendation to Congress (June 2005) ("2005 SAFE WEB Act Proposal"), https://www.ftc.gov/sites/default/files/documents/reports/us-safe-web-act-protecting-consumers-spam-spyware-and-fraud-legislative-recommendation-congress/ussafeweb.pdf.
[45] 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)), available at http://uscode.house.gov/statutes/pl/109/455.pdf.
[46] Sections 4(a) and 6(a) of the SAFE WEB Act codified at Sections 6(f) and 21(b)(6) of the FTC Act, 15 U.S.C. §§ 46(f) and 57b-2(b)(6).
[47] Section 4(b) of the SAFE WEB Act codified at Section 6(j) of the FTC Act, 15 U.S.C. §46(j).
[48] Section 6(b) of the SAFE WEB Act codified at Section 21(f) of the FTC Act, 15 U.S.C. § 57b-2(f).
[49] Section 3 of the SAFE WEB Act codified at Section 5(a)(4) of the FTC Act, 15 U.S.C. § 45(a)(4).
[50] Section 9 of the SAFE WEB Act codified at Section 25A of the FTC Act, 15 U.S.C. § 57c-1.
[51] The U.S. SAFE WEB Act: The First Three Years. A Report to Congress (Dec. 2009), https://www.ftc.gov/reports/us-safe-web-act-first-three-years-federal-trade-commission-report-congress.
[52] Commission Letter to the Honorable John D. Rockefeller IV, Kay Bailey Hutchinson, Mark Pryor, and Patrick J. Toomey, United States Senate Committee on Commerce, Science and Transportation (Oct. 3, 2011) and Commission Letter to the Honorable Fred Upton, Henry Waxman, Mary Bono Mack, and G.K. Butterfield, U.S. House of Representatives Committee on Energy and Commerce (Oct. 3, 2011), https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/repeal-sunset-provision-us-safe-web-act-2006).

renewing the Act, set to expire in December 2013; [53] Congress renewed the Act in 2012 for an additional seven years.[54] In October 2019, all five FTC Commissioners again urged Congress to reauthorize the Act.[55] In 2020, Congress renewed SAFE WEB for an additional seven years.[56] SAFE WEB is currently set to expire on September 30, 2027.[57]

B. Cross-Border Enforcement Cases

SAFE WEB affirmed the FTC's authority to pursue harms that cause reasonably foreseeable injury or involve material conduct here in the U.S.[58] As detailed in Appendix C, the FTC has initiated at least 145 enforcement actions with a public cross-border component since Congress passed SAFE WEB. These cases, which in many instances involve some aspect of cross-border cooperation, constitute some of the FTC's most important work since the FTC last reported to Congress on SAFE WEB.

SAFE WEB affirmed the FTC's ability to act upon unfair and deceptive practices involving foreign commerce that have sufficient relation to the U.S., and the FTC has vigorously pursued this mandate.[59] The FTC has conducted more than **450 investigations** with international components, such as foreign targets, evidence, or assets. Many of these investigations involved cross-border complaints.

The examples below highlight how the FTC has acted upon cross-border complaints[60] and the importance of having clear legislative authority to protect the public both within the U.S. and abroad, by pursuing matters with cross-border components.

In re Sanctuary Belize

SAFE WEB's clear grant of extraterritorial authority allowed the FTC to stop one of the largest overseas real estate investments scams targeting U.S. consumers and ultimately obtain funds for consumer redress that it might not have been able to do otherwise. In 2018, at the FTC's request, a federal district court in Maryland issued an order temporarily shutting down the scheme, known by several names, including "Sanctuary Belize," which took in more than $100 million marketing lots in what supposedly would

---

[53] July 2012 Prepared Statement of Hugh Stevenson, https://www.ftc.gov/legal-library/browse/prepared-statement-federal-trade-commission-reauthorizing-us-safe-web-act-2006.
[54] Public L. No. 112-203, 126 Stat. 1484 (2012), available at https://www.congress.gov/112/plaws/publ203/PLAW-112publ203.pdf.
[55] Letter of the Federal Trade Commission to the U.S. House of Representatives, Subcommittee on Consumer Protection and Commerce on the U.S. SAFE WEB Act (Oct. 25, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-federal-trade-commission-us-house-representatives-subcommittee-consumer-protection-commerce.
[56] Public L. No. 116-173, 134 Stat. 837 (2020) (codified in part at 15 U.S.C. § 44), available at https://www.congress.gov/116/plaws/publ173/PLAW-116publ173.pdf.
[57] *Id*.
[58] Section 3 of the SAFE WEB Act codified at Section 5(a)(4) of the FTC Act, 15 U.S.C. § 45(a)(4) (defining the term "unfair or deceptive acts or practices" to include those that "(i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States").
[59] *Id*.
[60] Additional information about how the FTC uses and acts on complaints can be found in Appendix B.

become a luxury development in Central America.[61] The FTC obtained a judgment for over $100 million and settled with several of the defendants, including Belize's Atlantic International Bank Limited, which FTC alleged assisted various entities in deceiving U.S. consumers.[62] In August 2023, the FTC began the first phase of its redress efforts, sending refunds totaling approximately $10 million to 1,198 defrauded investors.[63]

MOBE Ltd.

SAFE WEB's extraterritorial authority and consumer complaints also helped the FTC shut down an international operation that targeted U.S. consumers, including service members and veterans, through a deceptive internet business coaching scheme called "My Online Business Education" – MOBE.[64] Relying in part on over 150 consumer complaints, the Commission sued MOBE in 2018.[65] The FTC alleged that the international operation, which was run by entities and individuals in Malaysia, Australia, Canada, and the U.K., targeted U.S. consumers through online ads, social media, direct mailers, and live events held throughout the country, and falsely claimed that its program would enable people to start their own online businesses and earn substantial income quickly and easily. In April 2022, the Commission returned over $23 million to victims who invested in the program.[66]

On Point Global LLC

The FTC's SAFE WEB authority and consumer complaints have also helped the FTC prevail on law enforcement actions in court. In February 2020, the FTC sued five individuals and more than 50 of their

---

[61] Ex Parte Temporary Restraining Order with Asset Freeze, Writs Ne Exeat, Appointment of Temporary Receiver, and Other Equitable Relief, and Order to Show Cause Why a Preliminary Injunction Should Not Issue, *In re Sanctuary Belize Litigation,* No. 1:18-cv-03309-PJM (D. Md., Oct. 31, 2018), ECF No. 13, available at https://www.ftc.gov/system/files/documents/cases/ecological_fox_tro.pdf. *See also* Press Release, FTC, At FTC's Request, Court Halts Massive "Sanctuary Belize" Real Estate Investment Scam, https://www.ftc.gov/news-events/news/press-releases/2018/11/ftcs-request-court-halts-massive-sanctuary-belize-real-estate-investment-scam.

[62] *See* Press Release, FTC, Belizean Bank to Pay $23 Million and Cease Operations to Settle FTC Charges It Provided Substantial Assistance to the Sanctuary Belize Real Estate Scam (Sept. 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/09/belizean-bank-pay-23-million-cease-operations-settle-ftc-charges-it-provided-substantial-assistance.

[63] *See* Press Release, FTC, FTC Sending Refunds to Consumers who Invested in Deceptive Sanctuary Belize Real Estate Development Scheme Operated by Repeat Offender Andris Pukke, (Aug. 16, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/08/ftc-sending-refunds-consumers-who-invested-deceptive-sanctuary-belize-real-estate-development-scheme?utm_source=govdelivery.

[64] *FTC v. MOBE Ltd.*, No. 6:18-cv-862-ORL-37DCI, (M.D. Fla. June 4, 2018). *See also* Press Release, FTC, FTC Action Halts MOBE, a Massive Internet Business Coaching Scheme (June 11, 2018), https://www.ftc.gov/news-events/news/press-releases/2018/06/ftc-action-halts-mobe-massive-internet-business-coaching-scheme.

[65] Plaintiff's Ex Parte Motion and Memorandum of Law in Support of a Temporary Restraining Order and Order to Show Cause why a Preliminary Injunction Should not Issue at 18*, FTC v. MOBE Ltd.*, No. 6:18-cv-862-ORL-37DCI, (M.D. Fla. June 4, 2018), ECF No. 3, available at https://www.ftc.gov/system/files/documents/cases/mobe_motion-memo_for_tro_not_file_stamped.pdf.

[66] *See* Press Release, FTC, Federal Trade Commission Returns More Than $23 Million To Consumers Deceived by Online Business Coaching Scheme MOB (Apr. 5, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/04/federal-trade-commission-returns-more-23-million-consumers-deceived-online-business-coaching-scheme.

companies for operating hundreds of fake government assistance websites.[67] The defendants included a call center in Costa Rica (which handled calls with U.S. consumers) and a web development office in Uruguay (which created content targeting consumers). The Court found, based in part on consumer complaints, that the FTC was likely to prevail on the merits of its cases and issued a preliminary injunction that, among other things, stopped the defendants from misrepresenting their services.[68] After winning at trial, the FTC made $102 million in refunds available to consumers who were harmed by the scheme.[69]

Next-Gen, Inc.

Through the use of SAFE WEB and consumer complaints, the FTC has also been able to seek effective relief for consumers in the U.S. and abroad simultaneously. In February 2018, in *FTC v. Next-Gen, Inc.*, the FTC and the State of Missouri charged two men and their sweepstakes operation with scamming tens of millions of dollars from consumers throughout the U.S. and other countries, including Canada, the U.K., France, and Germany.[70] The FTC and Missouri alleged that the defendants, operating from the U.S. under dozens of different names, sent tens of millions of personalized mailers falsely indicating that the recipient had won or was likely to win a substantial cash prize in exchange for a fee ranging from $9 to $139.99, resulting in losses of more than $110 million. Consumer complaints showed the extent to which the defendants had deceived consumers in various countries for years. The FTC settled with the defendants, permanently banning them from the prize promotion business,[71] and sent nearly $25 million to consumers who were defrauded by the scheme.[72] While most redress went to consumers in the U.S. and Canada, who received checks totaling $19,180,753, the FTC – in cooperation with several foreign counterparts – also sent debit cards totaling $631,322 to consumers in the U.K., and letters to consumers in more than 50 other countries explaining how they could claim their payments via PayPal, which totaled $4,696,242.

---

[67] *FTC v. On Point Global LLC*, No. 19-cv-25046 (S.D. Fla. Dec. 9, 2019). *See also* Press Release, FTC, Court Stops Sprawling Scheme That Operated Hundreds of Websites That Deceived Consumers About Government Services (Fed. 5, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/02/court-stops-sprawling-scheme-operated-hundreds-websites-deceived-consumers-about-government-services.

[68] Plaintiff's Ex Parte Motion for a Temporary Restraining Order and Memorandum in Support Thereof at 3 and Order Granting Motion for Preliminary Injunction, *FTC v. On Point Global LLC*, No. 19-cv-25046 (S.D. Fla. Dec. 9, 2019), ECF Nos. 4 and 126, available at https://www.ftc.gov/system/files/documents/cases/on_point_tro_memorandum.pdf and https://www.ftc.gov/system/files/documents/cases/revenue_path-on_point_global_llc_preliminary_injunction.pdf.

[69] *See* Press Release, FTC, FTC Win at Trial Against On Point Global Makes $102 Million in Refunds Available for Consumers Harmed by Fake Government Website Scams (Apr. 7, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/04/ftc-win-at-trial-against-on-point-global-makes-102-million-in-refunds-for-consumers.

[70] *FTC v. Next-Gen, Inc., No. 4:18-CV-0128* (W.D. Mo. Feb. 20, 2018). *See also* Press Release, FTC, FTC Challenges Schemes That Target or Affect Senior Citizens (Feb. 22, 2018), https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-challenges-schemes-target-or-affect-senior-citizens.

[71] *See* Press Release, FTC, Operators of Sweepstakes Scam Will Forfeit $30 Million to Settle FTC Charges, https://www.ftc.gov/news-events/news/press-releases/2019/03/operators-sweepstakes-scam-will-forfeit-30-million-settle-ftc-charges.

[72] *See* Press Release, FTC, U.S. Federal Trade Commission Returning Almost $25 Million to Consumers Worldwide Who Were Defrauded by Next-Gen Sweepstakes Scheme (July 19, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/07/us-federal-trade-commission-returning-almost-25-million-consumers-worldwide-who-were-defrauded-next.

Fashion Nova, Inc.

Similarly, after cross-border complaints helped alert the FTC to the harmful practices of an international online retailer, the FTC relied on its SAFE WEB authority to enjoin the company's practices and obtain refunds for its customers. In 2020, in *FTC v. Fashion Nova, Inc.*, the FTC settled allegations that Fashion Nova violated the FTC's Mail, Internet, or Telephone Order Merchandise Rule (16 C.F.R. Part 435).[73] According to the FTC, Fashion Nova marketed and sold clothing and accessories to consumers in the U.S. and many other countries, but failed to properly notify consumers and give them the chance to cancel their orders when it did not ship their merchandise in a timely manner. The FTC received thousands of complaints about Fashion Nova's practices from U.S. consumers, and hundreds from consumers in Canada and more than fifty other countries. Pursuant to an FTC settlement, Fashion Nova refunded $2.26 million directly to consumers. The FTC also sent more than $6.5 million to injured consumers, mostly in the U.S., but also including more than $500,000 to consumers in 169 other countries.[74] This kind of result amplifies the deterrent effect on firms contemplating similar conduct.

Best Priced Brands, LLC

Although the FTC primarily employs SAFE WEB to protect U.S. consumers, SAFE WEB also clarifies and strengthens the FTC's ability to bring actions against U.S. companies even when their actions affect only foreign consumers. In 2009, the FTC pursued its first action against a U.S. company doing business exclusively with foreign consumers. The FTC sued Balls of Kryptonite, LLC, and its owner Javian Karnani (all doing business as Best Priced Brands and Bite Size Deals) after learning of a series of cross-border complaints against the entities.[75] Best Priced Brands, a California-based online electronics retailer, sold electronic products to consumers in the U.K., misleading them into believing that they were purchasing items from a U.K.-based company. Many U.K. consumers filed complaints through econsumer.gov noting they had been charged unexpected import duties and were told they would be charged high cancellation and refund fees if they attempted to return the merchandise. The FTC, following assistance by the U.K. Office of Fair Trading ("OFT"), filed suit in the U.S. District Court for the Central District of California, ultimately reaching a settlement with the defendants curbing such deceptive practices.[76] By going after scammers in the U.S. who harm consumers abroad, the FTC is able to protect the integrity and reputation of the U.S. market, and encourage reciprocal assistance from foreign enforcers.

---

[73] *FTC v. Fashion Nova, Inc.*, No. 2:20-cv-3641 (C.D. Cal. Apr. 20, 2020). *See also* Press Release, FTC, Fashion Nova Will Pay $9.3 Million for Consumer Refunds To Settle FTC Charges It Violated Rules On Shipping, Refunds (Apr. 21, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/04/fashion-nova-will-pay-93-million-consumer-refunds-settle-ftc-charges-it-violated-rules-shipping.

[74] *See* Press Release, FTC, FTC Sends More Than $6.5 Million to Consumers Harmed by Fashion Nova (Mar. 25, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/03/ftc-sends-more-65-million-consumers-harmed-fashion-nova.

[75] *FTC v. Javian Karnani*, No. 09-CV-5276 (C.D. Cal. July 20, 2009). *See also* Press Release, FTC, Court Halts U.S. Internet Seller Deceptively Posing as U.K. Home Electronics Site (Aug. 6, 2009), https://www.ftc.gov/news-events/news/press-releases/2009/08/court-halts-us-internet-seller-deceptively-posing-uk-home-electronics-site.

[76] *See* Press Release, FTC, FTC Settlement Bans Online U.S. Electronics Retailer from Deceiving Consumers with Foreign Website Names (June 9, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/06/ftc-settlement-bans-online-us-electronics-retailer-deceiving-consumers-foreign-website-names.

CafePress

The ability to bring such actions is also the cornerstone of our role in enforcing the substantive provisions of international data transfer programs enabling trillions of dollars in cross-border commerce, such as the European Union ("EU")-U.S. Data Privacy Framework (the successor to the Privacy Shield and Safe Harbor programs)[77] and the Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules System.[78] In these programs, U.S. companies can voluntarily make commitments on the treatment of data in order to enable its transfer from various foreign countries; those commitments then become enforceable as a matter of U.S. law under the FTC Act, as amended by SAFE WEB. One example of such a case is *CafePress*, in which the FTC alleged that the U.S. defendant, a participant in the EU-U.S. Privacy Shield program, did not comply with its commitments to provide EU consumers with the framework commitments as to choice, security, and access.[79]

SAFE WEB's explicit affirmation of the FTC's authority to pursue matters involving foreign commerce has helped the FTC prevail against jurisdictional challenges in many of the matters discussed above.[80] Thus, the Act constitutes a crucial component of the FTC's ability to effectively combat cross-border fraud, as well as other cross-border misconduct, that harms U.S. consumers.

C. Use of SAFE WEB Cooperation Tools

SAFE WEB gave the FTC the ability to share confidential or compelled information and to help foreign law enforcement agencies obtain U.S.-based evidence. These powers have been key in helping the FTC and foreign law enforcement cooperatively investigate to stop cross border fraud. Chief among these powers is the FTC's ability to share compelled or confidential information with and provide investigatory assistance to foreign law enforcement agencies.

As of June 30, 2023, the FTC has:

- Shared confidential or compelled information in response to **175** SAFE WEB sharing requests from **43** law enforcement agencies in **20** different countries.

---

[77] *See* U.S. Department of Commerce, Data Privacy Framework Program, EU-U.S. Data Privacy Framework and letter from Lina M. Khan, Chair of the Federal Trade Commission, Didier Reynders, Commissioner for Justice, European Commission (June 9, 2023), https://www.dataprivacyframework.gov/s/framework-text (last accessed Sept. 28, 2023).
[78] *See* Cross Border Privacy Rules System, https://cbprs.org/ (last accessed Sept. 28, 2023).
[79] *In the Matter of Residual Pumpkin, LLC (formerly d/b/a CafePress)*, Nos. C-4768, C-4769 (Mar. 15, 2021), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter; *See also In the Matter of Flo Health, Inc.*, No. C-4747 (Jan. 13, 2021), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc (alleging that Flo Health did not comply with Privacy Shield commitments to provide E.U. consumers with notice, choice, and accountability for onward transfers).
[80] *See*, *e.g.*, *In re Sanctuary Belize*, 482 F. Supp. 3d 373, 396 n.19 (D. Md. Aug. 28, 2020) (finding that the U.S. SAFE WEB Act decreed that the FTC Act and the Telemarketing Sales Rule apply extraterritorially, and that the Defendants' deceptive marketing to U.S. residents "causes or is likely to cause reasonably foreseeable injury" and that "extensive material conduct of Defendants occurred within the United States"), available at https://www.ftc.gov/system/files/documents/cases/1020_memorandum_opinion.pdf.

- Helped its foreign enforcement partners, both civil and criminal, to obtain U.S.-based evidence by issuing more than **140** CIDs in **67** investigations on behalf of **21** foreign agencies from **eight** countries.

Notably, the FTC has increasingly made active use of these tools. The activity described above includes ***more than 150*** **additional information sharing requests** and ***more than 110*** **additional CIDs** since the FTC reported to Congress on its experience using the U.S. SAFE WEB Act in 2009.[81]

Of critical importance, SAFE WEB cooperation often provides foreign counterparts with evidence that helps them to fight conduct affecting U.S. consumers.[82] Such cooperation has also encouraged reciprocal assistance from other countries, including through MOUs. Even more, SAFE WEB has established the FTC as a global example of effective cross-border cooperation in consumer protection matters[83] and encouraged other countries to adopt similar domestic legislation, to the benefit of the U.S. For example, in 2010, Canada passed anti-spam legislation with mutual assistance provisions modeled on the SAFE WEB Act.[84] The FTC has also been able to grow our relationships with other agencies, helping to advance the mutual cause of protecting consumers through more than a decade of staff exchanges.

---

[81] The work of law enforcement is often non-public and law enforcement agencies, both foreign and domestic, do not necessarily report back to the FTC on the results of FTC cooperation, including whether a foreign agency has engaged in an enforcement action. Examples of important public enforcement results obtained by foreign law enforcement and of which the FTC is aware are nevertheless provided in this report.

[82] Many of the cases tackled by the Canadian regional partnerships, for example, have involved Canada-based telemarketers targeting U.S. victims. Other cases pursued by foreign enforcers have involved both U.S. and foreign victims.

[83] *See generally* Organisation for Economic Cooperation and Development, Implementation toolkit on legislative actions for consumer protection enforcement co-operation (June 17, 2021), https://www.oecd.org/digital/implementation-toolkit-on-legislative-actions-for-consumer-protection-enforcement-co-operation-eddcdc57-en.htm. The toolkit is a "practical resource for consumer protection enforcement agencies that do not currently have the domestic legal authority needed for enforcement co-operation to make the case for obtaining relevant legislative tools." *Id.* at 2.

[84] An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23), available at https://laws-lois.justice.gc.ca/eng/acts/E-1.6/index.html). *See also* https://fightspam-combattrelepourriel.ised-isde.canada.ca/site/canada-anti-spam-legislation/en. Remarking on the legislation at the FTC's 2019 International Hearings on Competition and Consumer Protection in the 21st Century, CBC Commissioner Matthew Boswell commented that "[O]ur legal framework and ability to assist and share information with our foreign counterparts has improved significantly with the enactment of Canada's Anti-Spam Law, or 'C-A-S-L.' 'C-A-S-L' recently brought into force new express provisions allowing the Bureau to use our investigative powers under the Competition Act or Criminal Code to assist foreign partners, without us having to be conducting our own investigation. It grants these powers with the provision that information will only be used for that investigation or proceeding and will be kept confidential, similar to provisions in the U.S. Safe Web Act."

1. Sharing of Confidential and Compelled Information with Foreign Agencies

SAFE WEB authorizes the FTC to share information with foreign law enforcement agencies.[85] Importantly, SAFE WEB permits the FTC to share certain confidential and compelled information in its consumer protection investigations, upon certification by the foreign agency that the material will be maintained in confidence and used only to investigate or engage in enforcement proceedings related to "possible violations of . . . foreign laws prohibiting fraudulent or deceptive commercial practice, or other practices substantially similar to practices prohibited by any law administered by the Commission."[86] This standard permits the FTC to share with criminal as well as civil authorities, so long as the practices in question are "substantially similar." Prior to Congress passing the Act, the FTC could only share this information with U.S. enforcers. FTC procedures for handling requests from foreign law enforcement agencies are implemented in Commission Rule 4.11(j).[87]

The FTC has responded to **175** SAFE WEB information sharing requests from **43** law enforcement agencies in **20** different countries. A list of the agencies with which the FTC has shared non-public information pursuant to the Act since 2012 is set forth in *Figure 4*. This has included sharing compelled and confidential information related to foreign matters involving, for example, robocalls, text message spam, false advertising, data breaches, and sweepstake scams. Without SAFE WEB, sharing key enforcement information with these important partners would have been barred under the FTC Act.

Figure 4: SAFE WEB Information Sharing Agencies

Name of Agency	Country
Australian Competition and Consumer Commission	Australia
Australian Communications and Media Authority	Australia
Office of the Australian Information Commissioner	Australia
Federal Ministry for Social Affairs, Health Care, and Consumer Protection	Austria
BG Directorate-General for Economic Inspection	Belgium
Bulgarian National Bank	Bulgaria
Alberta Justice	Canada

[85] SAFE WEB Act Sections 4(a) and 6(a) codified in Sections 6(f) and 21(b)(6) of the FTC Act, 15 U.S.C. §§ 46(f) and 57b-2(b)(6)). "Foreign Law Enforcement Agency" means "any agency or judicial authority of a foreign government, including a foreign state, or a multinational organization constituted by and comprised of foreign states, that is vested with law enforcement or investigative authority in civil, criminal, or administrative matters" and "any multinational organization, to the extent that it is acting on behalf of" any such agency or judicial authority. SAFE WEB Act Section 2 codified in Section 4 of the FTC Act, 15 U.S.C. § 44.

[86] *Id*. Antitrust laws enforced by the FTC are not covered by the provisions. 15 U.S.C. §§ 46(f)(2) and 57b-2(b)(6). The Act also does not authorize the FTC to share information with agencies from countries that the Secretary of State has determined repeatedly support international terrorism. 15 U.S.C. § 57b-2(b)(6)(D). This prohibition also applies to agencies submitting requests for investigative assistance. 15 U.S.C. § 46(j)(7).

[87] 16 C.F.R. §4.11(j).

British Columbia Consumer Protection	Canada
Competition Bureau	Canada
Canadian Radio-television and Telecommunication Commission	Canada
Edmonton Police Service	Canada
Health Canada	Canada
Kahnawake Mohawk Peacekeepers	Canada
Ministry of the Attorney General (Ontario, Canada)	Canada
Ontario Provincial Police	Canada
Office of the Privacy Commissioner of Canada	Canada
Royal Canadian Mounted Police	Canada
Service Alberta	Canada
Toronto Police Service	Canada
York Police	Canada
Superintendency of Industry and Commerce	Colombia
Ministry of Commerce	Cyprus
Office of the Communication Authority	Hong Kong
Competition and Consumer Protection Commission	Ireland
Israel Consumer Protection and Fair Trade Authority	Israel
Consumer Affairs Agency	Japan
Korea Communications Commission	Korea
Luxembourg National Data Protection Commission	Luxembourg
Netherlands Independent Post and Telecommunications Authority	Netherlands
New Zealand Department of Internal Affairs	New Zealand
National Privacy Commission	Philippines
Singapore Police	Singapore
State Secretariat for Economic Affairs	Switzerland
City of London Police	U.K.
Competition and Markets Authority	U.K.
Financial Conduct Authority	U.K.
Information Commissioner's Office	U.K.
UK Insolvency Service	U.K.
Office of Fair Trading	U.K.
Serious Organised Crime Agency	U.K.
Staffordshire County Council	U.K.
Trading Scams Team	U.K.
Security Service Ukraine	Ukraine

Such information sharing activities with foreign law enforcement agencies have supported the FTC's enforcement efforts in many cases, including the following:

Designer Brand Outlet

Actions taken by the Australian Competition and Consumer Commission ("ACCC") against Designer Brand Outlet, with assistance from the FTC and the U.K.'s OFT, is an early example of how sharing information benefits consumer protection enforcement. Leading up to August 2008, consumers from around the world had complained that www.designerbrandoutlet.com, which purported to sell genuine, designer-label goods, had not delivered ordered goods, had delivered counterfeit goods, and had failed to provide refunds after consumers returned non-conforming goods. The FTC, having identified a series of complaints in econsumer.gov, notified the ACCC and, with the U.K.'s OFT, assisted the ACCC in investigating the scam. In late August 2008, having been contacted by the ACCC about the complaints, the Australian domain registrar NetRegistry Pty Ltd quickly disabled the domain name. In early September 2008, the ACCC filed proceedings against www.designerbrandoutlet.com and related individuals operating from China for false and misleading representations, obtaining an ex parte injunction freezing their assets and suspending their operations.[88] An Australian court found in favor of the ACCC in December 2008 and ordered compensation hearings (to provide redress to individual consumers).[89]

Ashley Madison

In 2016, the operators of the Toronto-based AshleyMadison.com dating site agreed to settle FTC charges that they deceived consumers and failed to protect 36 million users' account and profile information in relation to a massive July 2015 data breach of their network.[90] The website had users from over 46 countries. The FTC relied on key provisions of the SAFE WEB Act to share information with the Office of the Privacy Commissioner of Canada ("OPC") and the Office of the Australian Information Commissioner ("OAIC"), which reached their own settlements with the company and also contributed to the FTC's investigation. In 2017, the three agencies received an award for their cross-border investigation of the data breach from the Chair of what is now known as the Global Privacy

---

[88] *See* Press Release, Australian Competition and Consumer Commission, 'Designer Brand Outlet' website suspended (Sept. 9, 2008), https://www.accc.gov.au/media-release/designer-brand-outlet-website-suspended and Press Release, Australian Competition and Consumer Commission, Were you misled by Designer Brand Outlet? (Sept. 19, 2008) https://www.accc.gov.au/media-release/were-you-misled-by-designer-brand-outlet.

[89] *See* Press Release, Australian Competition and Consumer Commission, Court declares operators of Designer Brand Outlet website misled consumers (Dec. 15, 2008), https://www.accc.gov.au/media-release/court-declares-operators-of-designer-brand-outlet-website-misled-consumers and Press Release, Australian Competition and Consumer Commission, Refunds for some consumers who bought from Designer Brand Outlet (Apr. 28, 2009), https://www.accc.gov.au/media-release/refunds-for-some-consumers-who-bought-from-designer-brand-outlet.

[90] *FTC v. Ruby Corp.*, No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016). *See* Press Release, FTC, Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information (Dec. 14, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting-2015-data-breach-exposed-36-million.

Assembly, who called the agencies' work "a model on how to achieve cross-border cooperation in privacy enforcement."[91]

Foreign Money Offer Scams/MoneyGram/Western Union

Cross-border complaints, and a cooperative enforcement approach fostered by the U.S. SAFE WEB Act, helped the FTC work with foreign law enforcement agencies to stop a large criminal network. In 2013 and 2014, the FTC shared consumer complaints regarding fraudulent money transfers to Western Union and MoneyGram locations in Spain in connection with a Nigerian email scam. The scam, which involved spamming consumers with emails and persuading them to pay large sums of money for future financial rewards that never materialized, resulted in consumers, mostly in the U.S. and Canada, sending over $15 million to transfer booths across Spain in 2011 and 2012. Ultimately, the FTC, U.S. criminal authorities, and the Canadian Anti-Fraud Centre shared consumer complaints with the Spanish National Police via Europol, and in July 2014 the Spanish National Police arrested 84 Western Union agents involved in the scam, 80% of whom were Nigerian citizens. In 2017, when the FTC sued Western Union for failing to put in place effective anti-fraud policies and procedures, it cited this as one of several examples of Western Union's failing to act promptly against problem agents.[92] Western Union ultimately forfeited $586 million to the FTC and the Justice Department, and the FTC distributed approximately $300 million to redress victims.[93]

FTC v. Jesse Willms

In 2011, the FTC used SAFE WEB to help stop a multi-million dollar cross-border scam that injured more than four million U.S. consumers. In *FTC v. Jesse Willms*, the FTC sued the operators of an online operation that the FTC alleged lured consumers into "free" or "risk free" offers for various products that supposedly required only small shipping and handling fees.[94] The scam's operators, having obtained consumers' credit or debit card account numbers, then charged consumers substantial monthly recurring fees and often failed to provide refunds despite a money-back guarantee. The FTC alleged the defendants, mostly located in Canada, took in more than $467 million from consumers in the U.S., Canada, the U.K., Australia, and New Zealand, with most of the injured consumers residing in the U.S.

---

[91] *See* Press Release, FTC, FTC Earns Prestigious International Award for AshleyMadison.com Data Breach Investigation (Sept. 27, 2017), https://www.ftc.gov/news-events/news/press-releases/2017/09/ftc-earns-prestigious-international-award-ashleymadisoncom-data-breach-investigation.

[92] *FTC v. Western Union Co.*, No. 1:17-cv-00110-CCC (M.D. Pa. Jan. 19, 2017). *See also* Press Release, FTC, Western Union Admits Anti-Money Laundering Violations and Settles Consumer Fraud Charges, Forfeits $586 Million in Settlement with FTC and Justice Department (Jan. 19, 2017), https://www.ftc.gov/news-events/news/press-releases/2017/01/western-union-admits-anti-money-laundering-violations-settles-consumer-fraud-charges-forfeits-586.

[93] *See* FTC, Western Union Refunds (Sept. 2023), https://www.ftc.gov/enforcement/refunds/western-union-refunds.

[94] *FTC v. Jesse Willms*, No. 2:11-CV-00828 (W.D. Wash. May 16, 2011). *See also* Press Release, FTC, FTC Charges Online Marketers with Scamming Consumers out of Hundreds of Millions of Dollars with 'Free' Trial Offers (May 17, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/05/ftc-charges-online-marketers-scamming-consumers-out-hundreds-millions-dollars-free-trial-offers.

The FTC worked closely with Canadian law enforcement, including the Alberta Partnership Against Cross Border Fraud,[95] in investigating this international scheme.[96] The FTC used SAFE WEB's information sharing provisions to share information with Canadian law enforcers, including the Competition Bureau Canada and the Royal Canadian Mounted Police ("RCMP"), which in turn provided investigative assistance to the FTC. The case resulted in the entry of U.S. court injunctions and monetary judgments, including a $359 million judgment and permanent ban against twelve defendants.[97]

In re Cambridge Analytica, LLC

The FTC used SAFE WEB to share information with the U.K.'s Information Commissioner's Office ("ICO") concerning Cambridge Analytica. Both agencies were investigating Cambridge Analytica for having harvested personal information from millions of Facebook users. In October 2018, the ICO fined Facebook £500,000.[98] In July 2019, the FTC sued Cambridge Analytica and filed settlements with the company's former CEO and an app developer. The ICO's Deputy Commissioner called the use of these information-sharing powers a "huge positive" in cross-border case cooperation.[99]

Next-Gen, Inc.

The FTC has also used its SAFE WEB information sharing authority to help redress injured consumers. In 2022, in *FTC v. Next-Gen* (*see* Section III, *supra*), the FTC shared information from its files with foreign agencies to help facilitate redress to consumers in those countries. The FTC also worked closely with consumer protection counterparts in 18 countries to coordinate messaging so that victims would be more likely to act upon the FTC's information about claiming redress funds.

---

[95] *See* Memorandum of Understanding on the Establishment of a Joint Venture Between Alberta Government Services, Canada's Competition Bureau, United States Federal Trade Commission's Bureau of Consumer Protection, Royal Canadian Mounted Police, Calgary Police Service, Edmonton Police Service, and United States Postal Inspection Service on the Enforcement of Deceptive Marketing Practices Laws (Sept. 26, 2003), https://www.ftc.gov/system/files/attachments/international-competition-consumer-protection-cooperation-agreements/alberta_mou.pdf.

[96] *See* Press Release, FTC, FTC Halts Deceptive Practices of Marketer Who Collected $359 Million Using Bogus 'Free' Trial Offers (Feb. 23, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/02/ftc-halts-deceptive-practices-marketer-who-collected-359-million-using-bogus-free-trial-offers.

[97] *See* FTC, Willms, Jesse, et al. (Mar. 6, 2012), https://www.ftc.gov/legal-library/browse/cases-proceedings/102-3012-willms-jesse-et-al.

[98] *See* Information Commissioner's Office, Investigation into the use of data analytics in political campaigns, A report to parliament (Nov. 6, 2018) at 38, https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf.

[99] FTC Hearings on Competition and Consumer Protection in the 21st Century, Transcript from March 25, 2019 at 110, https://www.ftc.gov/system/files/documents/public_events/1454018/ftc_hearings_session_11_transcript_day_1_3-25-19_0.pdf.

First Consumers

In 2014, in *FTC v. First Consumers, LLC*, the FTC moved to shut down a multi-million-dollar telemarketing fraud that targeted seniors across the U.S.[100] The defendants, through a network of U.S. and Canadian entities, used a telemarketing boiler room in Canada to cold-call seniors. The defendants, impersonating government and bank officials, enticed consumers to disclose their confidential bank account information and then used that information to create checks drawn on consumers' bank accounts. Those funds were deposited into accounts in the U.S. and then transferred to accounts controlled by the Canadian defendants. The FTC shared information with and received valuable help throughout the case from the RCMP, which helped serve process on Canada-based defendants. This matter resulted in the ringleader of the fraud being permanently banned from all telemarketing activities and a judgment of $10.7 million.[101]

As these examples demonstrate, SAFE WEB has been critical to stopping scams and other practices that have harmed consumers around the world, but especially in the U.S. This includes stopping scams that have caused significant financial injury. SAFE WEB has also provided for more effective parallel investigations and helped the FTC to provide redress to injured consumers. Finally, sharing information with our foreign law enforcement partners makes them more willing and able to share information with us.

2. Investigative Assistance to Foreign Law Enforcement Agencies

SAFE WEB also authorizes the FTC to provide investigative assistance to foreign law enforcement agencies.[102] The Act authorizes the Commission to "conduct such investigation as the Commission deems necessary to collect [pertinent] information and evidence. . . using all investigative powers authorized by [the FTC Act]" if certain criteria are met.[103] SAFE WEB also authorizes the FTC to initiate proceedings in federal district court pursuant to 28 U.S.C. § 1782 on behalf of foreign agencies to obtain testimony, documents, or things for use in foreign proceedings.[104]

Congress set forth certain requirements when the FTC provides investigative assistance to foreign law enforcement agencies. First, in a written request, the foreign agency must state that it is investigating or engaging in enforcement proceedings against "possible violations of laws prohibiting fraudulent or deceptive commercial practice, or other practices substantially similar to practices prohibited by any provision of the laws administered by the Commission (other than federal antitrust laws) . . ." In addition, in deciding whether to provide such assistance, the Commission must consider all relevant

---

[100] *FTC v. First Consumers, LLC*, No. 14-CV-1608 (E.D. Pa. March 18, 2014). *See also* Press Release, FTC, FTC Stops Mass Telemarketing Scam That Defrauded U.S. Seniors and Others Out of Millions of Dollars (Mar. 31, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/03/ftc-stops-mass-telemarketing-scam-defrauded-us-seniors-others-out-millions-dollars.

[101] *See* Press Release, FTC, Court Orders Ringleader of Scam Targeting Seniors Banned From Telemarketing (Mar. 12, 2015), https://www.ftc.gov/news-events/news/press-releases/2015/03/court-orders-ringleader-scam-targeting-seniors-banned-telemarketing.

[102] Section 4(b) of the SAFE WEB Act codified in Section 6(f) of the FTC Act, 15 U.S.C. §46(j).

[103] 15 U.S.C. §46(j)(1)-(3).

[104] 15 U.S.C. §46(j)(2)(B).

factors, including (A) whether the agency has agreed to or will provide reciprocal assistance, (B) whether compliance would prejudice the public interest of the U.S., and (C) whether the requesting agency's investigation or proceeding "concerns acts or practices that cause or as likely to cause injury to a significant number of persons."[105]

The FTC has provided investigatory assistance by issuing more than **140** CIDs in **67** investigations on behalf of **21** foreign agencies from **eight** countries. All of the CIDs were issued pursuant to general or special resolutions approved by the FTC's Commissioners. A list of the agencies to which the FTC has provided investigatory assistance pursuant to SAFE WEB is set forth in *Figure 5*.

Figure 5: SAFE WEB Investigatory Assistance Agencies

Name of Agency	**Country**
Australian Competition and Consumer Commission	Australia
Australian Communications and Media Authority	Australia
Directorate-General for Economic Inspection	Belgium
Edmonton Police Service	Canada
Competition Bureau	Canada
Canadian Radio-television and Telecommunication Commission	Canada
Health Canada	Canada
Royal Canadian Mounted Police	Canada
Toronto Police Service	Canada
York Police	Canada
Office of the Communication Authority	Hong Kong
Consumer Affairs Agency	Japan
Netherlands Independent Post and Telecommunications Authority	Netherlands
New Zealand Department of Internal Affairs	New Zealand
National Privacy Commission	Philippines
State Secretariate for Economic Affairs	Switzerland
City of London Police	U.K.
Competition and Markets Authority	U.K.
Information Commissioner's Office	U.K.
Office of Fair Trading	U.K.
Staffordshire County Council	U.K.

The nature of these requests has varied. For example, in some instances, the FTC has issued compulsory process to domain registrars in connection with investigations into spam, fake reviews, phishing

[105] 15 U.S.C. §46(j)(3).

schemes, or the sale of health and weight-loss supplements. In other instances, it has issued compulsory process to telecommunication companies or VoIP providers in connection with matters involving robocalls or other telemarketing matters, including a telemarketing sweepstake scam affecting U.S. consumers. The FTC has also issued compulsory process for subscriber information in relation to banks or payment processors in connection with money-laundering and multi-level marketing 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. In many instances, the FTC's SAFE WEB assistance to foreign law enforcement agencies has helped those agencies to take action against foreign-based fraudsters victimizing U.S. consumers.

Some examples of how the FTC has used SAFE WEB's investigative assistance authority to issue compulsory process are highlighted below. These examples supplement those the FTC reported to Congress in 2009.[106]

- In 2014, the FTC provided SAFE WEB investigative assistance to assist the RCMP in its investigation of Banners Brokers, a massive online pyramid scheme based in Canada that targeted consumers in the U.S., Canada, and around the world. Ultimately, the Toronto Police (working with the RCMP) arrested two of Banners Brokers' three principals and charged them criminally for their participation in the $93 million scheme.[107]

- In September 2018, the FTC used its SAFE WEB authority to issue six CIDs to U.S. entities associated with the secondary-ticketing platform viagogo, based in Switzerland. Viagogo U.K. (and its Swiss parent) were the subject of an enforcement action brought by the U.K.'s Competition and Markets Authority ("CMA") for violating various consumer laws through its advertising and pricing representations.[108] The company produced information to the FTC, which it shared with the CMA. Before the FTC moved to compel the production of other, responsive information, the CMA secured a court order against viagogo by consent in November 2018, and the FTC withdrew its CIDs.[109]

In addition, when the FTC reported to Congress on SAFE WEB in 2009, it had not yet had the opportunity to use SAFE WEB to initiate proceedings on behalf of foreign agencies pursuant to 28 U.S.C. § 1782. That changed in 2014, when the FTC successfully obtained an order for documents and oral testimony from Aegis Mobile, LLC ("Aegis"), a U.S. corporation, for use by Canada's Competition

---

[106] 2009 SAFE WEB Report at 12-14.
[107] Kendra Mangione, Canadians Arrested in US$93 Million Pyramid Scheme, CTV News (Dec 9., 2015, 10:45am), https://www.ctvnews.ca/canada/canadians-arrested-in-us-93m-pyramid-scheme-1.2693136?cache=%3FclipId%3D64268. In 2017, both men pled guilty to operating a pyramid scheme under the Canada Competition Act.
[108] *See* FTC, In the Matter of September 13, 2018 Civil Investigative Demands Issued to viagogo, Inc.; viagogo Entertainment Inc.; Pugnacious Endeavors, Inc.; Grover Street, Inc.; and Grover Street Holdings, Inc. (Nov. 29, 2018), https://www.ftc.gov/legal-library/browse/cases-proceedings/petitions-quash/matter-september-13-2018-civil-investigative-demands-issued-viagogo-inc-viagogo-entertainment-inc-0 and Press Release, United Kingdom, CMA launches court action against viagogo (Aug. 31, 2018), https://www.gov.uk/government/news/cma-launches-court-action-against-viagogo.
[109] *See Competition and Markets Authority v. viagogo*, No. FS-2018-000011, Order, (Ch, Nov 27, 2018) (U.K.)., available at https://assets.publishing.service.gov.uk/media/5bffe2afe5274a0fae2c5397/CMA_v_Viagogo_Order_27.11.pdf.

Bureau ("CCB").[110] The CCB requested the FTC's assistance in obtaining evidence from Aegis for use in its investigation of and enforcement proceeding against various Canadian wireless companies alleged to have deceptively advertised certain premium cellular services.

The FTC used SAFE WEB to obtain an order from a U.S. federal district court on behalf of the CBC.[111] The order permitted the FTC to obtain oral and documentary testimony from Aegis, with the FTC ultimately obtaining documents and deposing two corporate representatives, and then sharing such information with the CCB. The CCB in turn obtained over $24 million in refunds for victims of these deceptive practices.[112] Commissioner Matthew Boswell of the CCB, one of the FTC's most longstanding international partners, has said that this assistance was "of tremendous assistance to the Bureau in advancing its case."[113]

3. International Cooperation Agreements

The FTC's ability to share information and offer investigation assistance to foreign law enforcement agencies through SAFE WEB has also resulted in reciprocal assistance and cooperation from other countries.

To further international cooperation, the FTC enters into international arrangements, agreements, and MOUs with consumer protection agencies around the world. In these arrangements and agreements, the FTC represents that it will endeavor to engage in enforcement cooperation and information sharing. These important representations rest on the cooperation the FTC can provide to agencies through the Act. Because many foreign law enforcement agencies require such arrangements to assist the FTC, SAFE WEB's cooperation tools have also increased assistance to the FTC, to the benefit of consumers. Without SAFE WEB, the assistance the FTC can offer other law enforcement agencies and, as a result, the reciprocal assistance that the FTC receives, would be more limited.

Based on the SAFE WEB powers, the FTC has expanded its international cooperation by entering into MOUs with consumer, privacy, and/or telecommunications authorities in Canada, Chile, Colombia, Ireland, Mexico, the Netherlands, Nigeria, Peru, the U.K., the APEC cross-border privacy rules system, and public authorities that are members of the Unsolicited Communications Enforcement Network (UCENet).[114] This includes, for example, the FTC's 2017 MOU on Consumer Fraud Enforcement

---

[110] *See In re Application of the FTC for an Order Pursuant to 28 U.S.C. § 1782 to Obtain Information from Aegis Mobille LLC on Behalf of the Competition Bureau, Canada, for use by Foreign Judicial Proceedings*, 2014 U.S. Dist. LEXIS 106214 (D. Md. Aug. 4, 2014), available at https://www.ftc.gov/system/files/documents/cases/aegis_2014-08-04_corrected_decision.pdf.

[111] *Id.*

[112] *See* Press Release, Canada, Bell customers to receive up to $11.82 million as part of Competition Bureau agreement (May 27, 2016), https://www.canada.ca/en/competition-bureau/news/2016/05/bell-customers-to-receive-up-to-11-82-million-as-part-of-competition-bureau-agreement.html.

[113] Speech, Canada, International cooperation in competition law: views from above the 49th parallel (Mar. 25, 2019), https://www.canada.ca/en/competition-bureau/news/2019/03/international-cooperation-in-competition-law-views-from-above-the-49th-parallel.html.

[114] Some FTC MOUs on the other hand were undertaken before the legislation took effect or are otherwise not based on those powers. Copies of the FTC's international cooperation arrangements are available at FTC, International Cooperation Agreements, https://www.ftc.gov/policy/international/international-cooperation-agreements (last accessed Sept. 28, 2023).

between the FTC and the RCMP, which expanded and strengthened the agencies' efforts to share information, engage in joint investigations, and combat cross-border fraud.

4. International Staff Exchanges

SAFE WEB also authorizes the FTC to participate in staff exchanges with foreign government agencies. SAFE WEB authorizes the FTC to employ on a temporary basis officers or employees of foreign government agencies. It also provides that FTC officers or employees may work on a temporary basis for appropriate foreign government agencies.[115] This provision in the Act applies to both competition and consumer protection activities.

The purpose of these staff exchanges, as the FTC noted in proposing such a provision, is to "improve international law enforcement cooperation in cross-border matters." As the FTC explained in proposing the Act in 2005, "Allowing foreign employees to work on FTC cases and investigations and have access to confidential material would help those employees learn about FTC investigative techniques and later adopt those techniques in their agency investigations. They could also provide significant help investigating joint cases involving evidence or witnesses located in their country."[116]

Through the FTC's International Fellows Program and SAFE WEB Interns Program, **133 foreign colleagues from 41 jurisdictions** have come to work alongside FTC staff in the agency's Bureaus of Competition, Consumer Protection, and Economics, and the Office of Policy Planning.[117] These Fellows work with FTC attorneys, economists, investigators, and other staff, generally for three to six months, participating in activities such as investigations and enforcement proceedings, and gaining first-hand experience of how the FTC carries out its mission.[118] After the program, they return to their home agencies, able to share what they have learned and to help improve cross-border cooperation through the relationships they have developed. In turn, the FTC gains insight into their home agencies' laws, enforcement actions and approaches. It helps all concerned find common ground despite the inevitable legal and cultural differences that exist between any two agencies.

---

[115] Section 9 of the SAFE WEB Act codified in section 25a of the FTC Act, 15 U.S.C. § 57c-1. Section 9 permits the FTC to "retain or employ officers or employees of foreign government agencies on a temporary basis as employees of the Commission." It also authorizes the FTC to "detail officers or employees of the Commission to work on a temporary basis for appropriate foreign government agencies."

[116] FTC, An Explanation of the Provisions of the US SAFE WEB Act, explanation-provisions-us-safe-web-act.pdf (last accessed Sept. 28, 2023) (provided in connection with the FTC's 2005 SAFE WEB Act Proposal, *supra* note 44). This explanation also noted, "The types of exchanges contemplated here would not involve exchanges in highly classified or sensitive areas. Indeed, the FTC is often pursuing the same targets as its foreign counterparts, and the ability to develop joint investigations and cases while a foreign employee is detailed to the FTC would be highly beneficial. The same reasoning applies in the antitrust area, and therefore, we recommend that this provision cover staff exchanges on both the competition and consumer protection sides of the FTC's mission." *Id*. at n.66.

[117] During their assignments, fellows and interns work under the direct supervision of FTC officials and do not perform inherently governmental functions. Since 2007, the FTC has hosted fellows and interns from Argentina, Australia, Austria, Barbados, Brazil, Canada, Chile, China, Columbia, Egypt, El Salvador, Ecuador, Egypt, the European Commission, France, the Gambia, Honduras, Hungary, India, Israel, Japan, Kazakhstan, Kenya, Lithuania, Mauritius, Mexico, Nigeria, Pakistan, Peru, the Philippines, Poland, Saudi Arabia, Singapore, South Africa, south Korea, Switzerland, Tanzania, Turkey, Ukraine, the U.K., Vietnam, and Zambia.

[118] SAFE WEB interns engage in similar work, but for shorter terms.

While the FTC has had more than ten times as many incoming SAFE WEB secondees as it has sent out, FTC employees have worked on **15** temporary SAFE WEB assignments to foreign government agencies since 2007.[119] FTC staff detailed to foreign government agencies similarly build relationships and gain valuable understanding of the policies and practices of foreign enforcement and policy agencies.

These staff exchanges—now almost 150 of them—have advanced the goal of cross-border cooperation to the benefit of U.S. law enforcement and consumers. Through these exchanges, the FTC and foreign competition, consumer protection, and privacy agencies have shared best practices, promoted better understanding of agency similarities and differences, and deepened their relationships. In addition, the understanding gained, and relationships built through these programs, have laid the groundwork for cooperation on later enforcement matters.

Photo 1 (Sunmi Lee of the Korea Fair Trade Commission with then-Commissioner William Kovacic.)

[119] FTC secondments abroad have included details with the European Commission and with agencies in Canada, the U.K., and Mexico. The FTC also has seconded staff to various agencies in developing countries in connection with USAID programs.

5. Other SAFE WEB Cooperation and Benefits

SAFE WEB permits the FTC to protect certain information from public disclosure, including certain confidential information obtained from foreign law enforcement and certain consumer complaints.[120] This helps to promote case information sharing that without such confidentiality protections might not otherwise occur. It also promotes foreign complaint contributions to Consumer Sentinel, contributing to cross-border law enforcement and providing greater insight into cross-border and international fraud.

SAFE WEB also authorizes the FTC, with the concurrence of the Attorney General, to designate Commission attorneys to assist the Attorney General in connection with litigation in foreign courts.[121] This provision has resulted in the FTC's close and frequent collaboration with the Department of Justice's Office of Foreign Litigation ("OFL"), which represents the FTC in its foreign litigation.[122] The FTC's collaboration with OFL – an excellent and important resource for FTC matters involving foreign service of process and obtaining evidence abroad – has benefitted numerous FTC domestic litigations.[123]

The ability to engage in foreign litigation has also benefited U.S.-based consumers. Our litigation to stop a debt reduction scam in *FTC v. E.M.A. Nationwide, Inc.*,[124] shows the potential for such action. Through participation in Canada regional partnerships, the FTC has nurtured its relationship with Canada law enforcement agencies, including in Montreal. These relationships led to cooperation, including the RCMP (facilitated by CBC's Montreal office) alerting the FTC that it had seized over $2 million in funds covered by an October 2012 FTC asset freeze. With key assistance from OFL, which represented the FTC's interest in the matter, Canada counsel was retained to seek judicial assistance from the Canada courts to repatriate the frozen funds to the U.S. In February 2013, a Quebec Court issued two Judgments granting the FTC's motions for judicial assistance to conserve the seized funds during the pendency of the FTC's U.S. action for the potential benefit of the victims. The FTC believes that these two judgments were the first time a Quebec court had granted this type of relief in aid of a U.S. preliminary injunction. As a result of the FTC's work with the RCMP and OFL, in December 2015, the FTC repatriated the frozen Canadian funds to the U.S. to benefit consumers via an FTC-administered redress program.[125]

III. Recommendations for Congress

We have two recommendations in this Report. First, that Congress should remove the sunset provision to the SAFE WEB Act and second that Congress should amend Section 13(b) of the FTC Act to restore

---

[120] Section 6(b) of the SAFE WEB Act codified at Section 21(f) of the FTC Act, 15 U.S.C. § 57b-2(f).
[121] Section 5 of the SAFE WEB Act codified at Section 16 of the FTC Act, 15 U.S.C. § 56.
[122] Since 2011, the FTC has had a staff member detailed to the OFL one day per week to represent the FTC's interests.
[123] For example, OFL recently assisted the FTC in hiring an expert on French attorney client privilege issues so that the FTC could more effectively respond to discovery objections. This assistance was instrumental in achieving a successful outcome in that dispute.
[124] *FTC v. E.M.A. Nationwide, Inc.*, No. 1:12-cv-2394 (N.D. Ohio Sept. 25, 2012). *See also* FTC, E.M.A. Nationwide, also d/b/a EMA and Expense Management America, et al. (May 9, 2016), https://www.ftc.gov/legal-library/browse/cases-proceedings/122-3069-ema-nationwide-also-dba-ema-expense-management-america-et-al.
[125] *See* Press Release, FTC, FTC Returns $1.87 Million to Consumers Harmed by Debt Relief Scam (May 9, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/05/ftc-returns-187-million-consumers-harmed-debt-relief-scam.

the FTC's ability to provide refunds to harmed consumers and prevent bad actors from keeping money generated by breaking the law.

Since Congress enacted SAFE WEB, FTC Commissioners have repeatedly and on a bipartisan basis recognized the Act's utility and encouraged Congress to make the legislation permanent.[126] If this legislation were to lapse, the FTC would lack what is now clear authority to pursue many matters relating to foreign commerce; this could have a dramatic negative impact on U.S. consumers.[127] In addition, the FTC's inability to help foreign partners would hinder its ability to obtain assistance from foreign partners. Moreover, many of the international data transfer mechanisms relied on by scores of businesses for cross-border commerce – such as the EU-U.S. Data Privacy Framework – would be called into question. As cross-border fraud and other misconduct continues to evolve and harm the public, it is imperative that Congress preserve the many important tools provided by the U.S. SAFE WEB Act, so that the FTC can continue to use those tools to protect the American public.

As demonstrated by the FTC's ample record of cross-border fraud enforcement set forth in this report, the ability to compensate fraud victims for their losses is a key part of the agency's work to protect American victims from foreign misconduct. Since 2017, the FTC cases have resulted in nearly 12 billion dollars returned to victims, including victims of conduct by foreign bad actors. These refunds also include over 14 million dollars sent to recipients in over 110 countries, encouraging similar initiatives from foreign counterparts.[128]

In addition, as the Commission has stated several times in prior congressional testimony, the FTC urges Congress to amend Section 13(b) of the FTC Act[129] to restore the FTC's ability to provide refunds to harmed consumers and prevent violators from keeping the money they earned by breaking the law. In April 2021, the Supreme Court issued its decision in *AMG Capital Management v. FTC*, which overturned four decades of circuit court precedent and held that Section 13(b) of the FTC Act no longer allowed courts to order defendants to pay refunds to harmed consumers or order defendants to disgorge their unjust gains.[130] That decision has significantly hampered the FTC's ability to get harmed consumers their money back and prevent wrongdoers from profiting from their violations of the FTC Act.[131] Restoring the FTC's ability to use Section 13(b) to obtain court orders requiring companies to

---

[126] *See supra* note 52. *See also*, Hearings on Competition and Consumer Protection in the 21st Century, The FTC's Role in a Changing World (Oct. 2020) at 5, https://www.ftc.gov/system/files/documents/reports/commission-report-hearings-competition-consumer-protection-21st-century/p181201internationalhearingreport.pdf.
[127] *See* Section II.B. *See, also*, *Morrison v. Nat'l Austl. Bank Ltd*, 561 U.S. 247, 254-262 (June 24, 2010) (upholding the presumption that, absent contrary Congressional intent, legislation does not have extraterritorial effect).
[128] *See* FTC Refunds to Consumers, https://public.tableau.com/app/profile/federal.trade.commission/viz/Refunds_15797958402020/RefundsbyCase (last accessed Sept. 26, 2023) (these total amounts include money returned to consumers directly by defendants or other third parties in certain cases). The U.S. SAFE WEB Act explicitly permits restitution to foreign victims of unfair or deceptive acts or practices if such relief is available to the Commission. 15 U.S.C. § 45(a)(4)(B).
[129] 15 U.S.C. § 53(b).
[130] *AMG Capital Mgmt., LLC v. FTC*, 141 S. Ct. 1341 (Apr. 22, 2021).
[131] *See, e.g.,* Press Release, FTC, FTC Order to Bar ZyCal Bioceuticals from Deceptive Health Marketing (Feb. 6, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-order-bar-zycalbioceuticals-deceptive-health-marketing

pay equitable monetary relief is critical to the agency's ability to protect consumers from cross-border fraud.

Conclusion

Cross-border fraud causes significant harm, with consumer reports alone indicating more than $5.2 billion in injury since 2015. And while often shifting, cross-border fraud shows no sign of abating. The U.S. SAFE WEB Act has equipped the FTC to better tackle cross-border fraud by affirming the FTC's authority to pursue harms that cause reasonably foreseeable injury or involve material conduct in the U.S. and allowing the FTC to cooperate with foreign law enforcement. It also supports trillions of dollars in cross-border commercial transactions. To preserve the FTC's ability to continue to protect American consumers from cross-border fraud and to help promote the exchange of data necessary for cross-border commerce, the FTC encourages Congress to make the U.S. SAFE WEB Act permanent. To restore the FTC's ability to provide refunds to injured consumers, the FTC also urges Congress to amend Section 13(b) of the FTC Act.

("Unfortunately, the Supreme Court decision in *AMG Capital Management* prevented us from obtaining refunds for consumers in this case. The Commission has urged Congress to enact legislation to restore the agency's ability to obtain critical relief for consumers through federal court actions."); Press Release, FTC, Federal Court Rules in Favor of FTC, Halting Illegal Tactics Used to Promote Smoking Cessation, Weight-Loss, and Sexual-Performance Aids (Mar. 25, 2022), https://www.ftc.gov/newsevents/news/press-releases/2022/03/federal-court-rules-favor-ftc-halting-illegal-tactics-used-promote-smokingcessation-weight-loss ("[D]espite the fact that the FTC presented evidence that consumers lost $18.2 million to the defendants' deceptive marketing, the court declined to order any compensation because of [the] Supreme Court's ruling in the case of *AMG v. FTC*, which undercuts the agency's authority to obtain such consumer redress.")

Acknowledgments

This report was drafted by Stacy Procter, Olivia Barney-Fishbein and Laureen Kapin of the FTC's Office of International Affairs. Additional acknowledgement goes to Paul Witt, Elizabeth Anne Miles, and Nicholas Mastrocinque of the FTC's Division of Consumer Response and Operations.

Appendix A

Additional Details on Cross-Border and International Fraud Data

Consumer complaints show that cross-border fraud is multifaceted, with U.S. and other consumers encountering fraud in various forms and from a multitude of sources. Between January 1, 2019 and June 30, 2023 (during which complete Sentinel data is currently available) some of the most common frauds that U.S. consumers encountered from foreign businesses related to such diverse issues as online shopping (e.g., undisclosed costs, failure to deliver on time, non-delivery, and refusal to honor a guarantee), impersonation fraud (e.g., romance, tech support, and business and family and friend imposter scams), unsolicited commercial emails (i.e., spam), miscellaneous investment scams (e.g., virtual currencies and investment advice and seminars), and computer exploits (e.g., spyware, adware, and malware). Of these frauds, two of the most prevalent reported during this period were **online shopping** and **romance scams**, with online shopping being the top complaint subcategory for *each* year between 2019 and 2022 and the first half of 2023, and romance scams being either the second or third top complaint subcategory each year (after excluding other miscellaneous complaints) and the first half of 2023. Statistics and data on the top 10 subcategories of cross-border fraud as reported by U.S. consumers for January 1, 2019, to June 30, 2023 (combined) is set forth in *Figure 6* below. (Data though 2022 is current as of August 22, 2023. *See* note 32, *supra*, for additional information on fraud reporting categories and subcategories.)

Figure 6: Top 10 Cross-Border Fraud Complaint Categories from U.S. Consumers

Rank	Sentinel Fraud Subcategory	Count	Percentage of Complaints
1	Online Shopping	80,659	29%
2	Other Misc.	40,380	14%
3	Romance Scams	30,003	11%
4	Business Imposters	19,866	7%
5	Misc. Investments & Investment Advice	16,724	6%
6	Tech Support Scams	13,840	5%
7	Unwanted Telemarketing	10,714	4%
8	Unsolicited Email	10,223	4%
9	Family & Friend Imposters	10,192	4%
10	Malware & Computer Exploits	9,135	3%

U.S. consumers also encounter different types of fraud from different countries. For example, in recent years, when reporting about fraud originating in China and Canada, the most common frauds reported

by U.S. consumers related to online shopping. Complaints by U.S. consumers about businesses in India largely involved imposter scams, such as tech support and business imposter scams. And while consumers in the U.S. often complain about online shopping frauds originating in the U.K., in 2021 and 2022 the most common frauds that U.S. consumers reported for companies located in the U.K. related to miscellaneous investments, such as investment opportunities in virtual currency and investment advice or seminars. Detailed data on the top ten fraud subcategories that U.S. consumers have experienced from different countries between 2019 and 2022 is provided in *Figure 7*.

Figure 7: Annual Top 10 Fraud Subcategories as Reported by U.S. Consumers

2019		
Country	Complaint Category	Complaint Total
China*	Online Shopping	5,731
Canada	Online Shopping	1,847
China*	Other Miscellaneous	1,442
India	Tech Support Scams	1,314
U.K.	Online Shopping	1,233
Canada	Other Miscellaneous	802
Jamaica	Miscellaneous Investments & Investment Advice	794
Jamaica	Advance-Fee Credit	773
Jamaica	Prizes, Sweepstakes & Lotteries	766
Nigeria	Romance Scams	753

2020		
Country	Complaint Category	Complaint Total
China*	Online Shopping	13,708
China*	Other Miscellaneous	10,798
Canada	Online Shopping	3,360
U.K.	Online Shopping	2,459
China*	Social Networking Services	1,138
Canada	Vacation & Travel	1,131
Mexico	Family & Friend Imposters	1,034
Jamaica	Prizes, Sweepstakes & Lotteries	938
Canada	Other Miscellaneous	857
Philippines	Romance Scams	799

2021		
Country	Complaint Category	Complaint Total
China*	Online Shopping	8,162
China*	Other Miscellaneous	7,203
Canada	Online Shopping	2,215
India	Business Imposters	1,864
India	Tech Support Scams	1,599
U.K.	Online Shopping	1,592

2022		
Country	Complaint Category	Complaint Total
China*	Online Shopping	4,321
U.K.	Miscellaneous Investments & Investment Advice	1,692
Canada	Online Shopping	1,551
China*	Other Miscellaneous	1,532
India	Tech Support Scams	1,508
India	Business Imposters	1,378

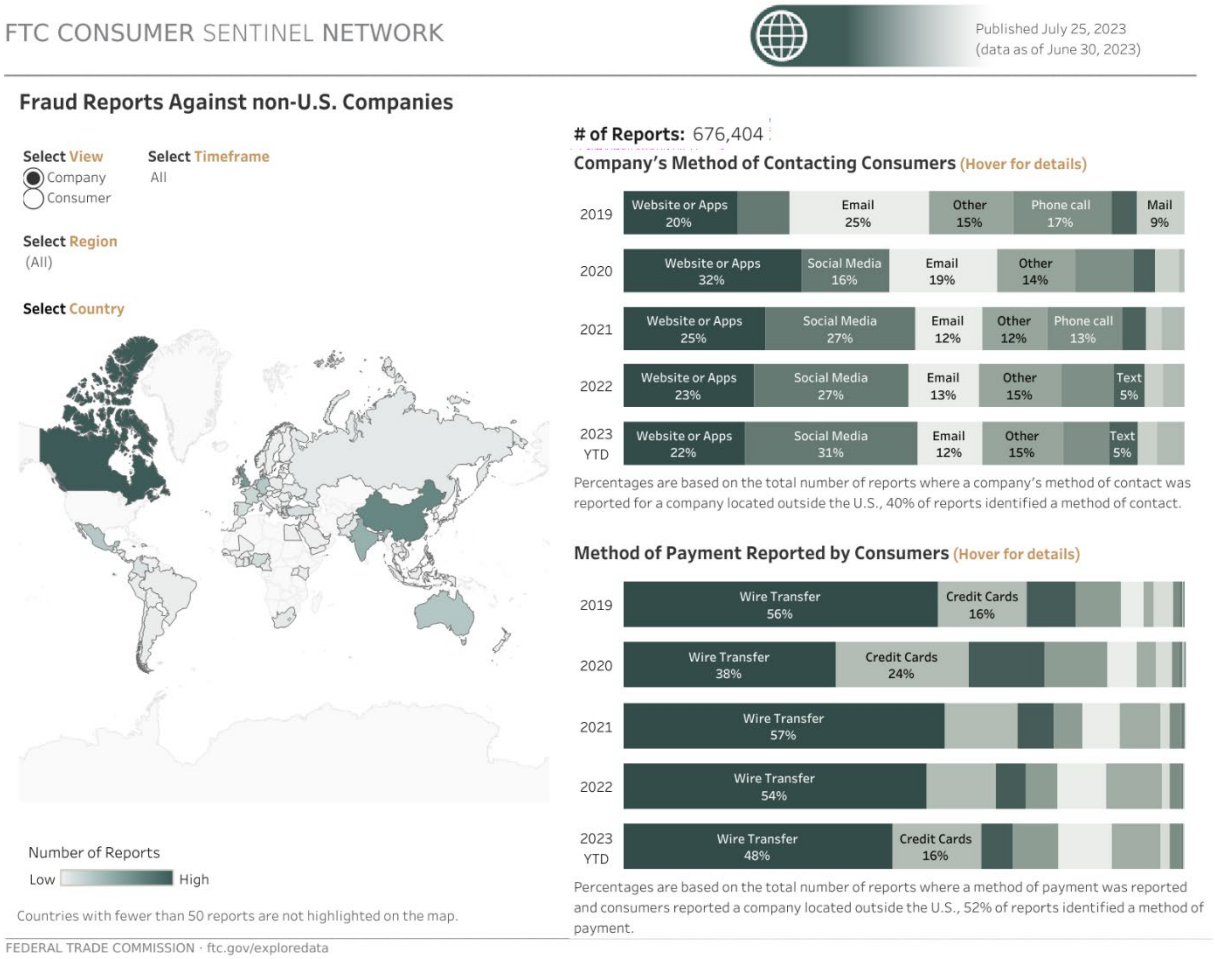
U.K.	Miscellaneous Investments & Investment Advice	1,453
India	Unwanted Telemarketing Calls	1,442
Mexico	Family & Friend Imposters	1,326
Philippines	Romance Scams	1,201

China*	Miscellaneous Investments & Investment Advice	1,320
U.K.	Online Shopping	1,162
Philippines	Malware & Computer Exploits	1,000
Canada	Vacation & Travel	998

(**China includes Hong Kong and Macau*.)

International fraud reports more generally (all complaints where the reported consumer or company is not from the U.S.) also suggest that in recent years consumers have increasingly been targeted by scammers outside of the U.S. through social media, websites, and apps. Since January 1, 2019, U.S. and foreign consumers collectively have reported a decrease in international fraud being initiated through email and the telephone, and a corresponding increase through other internet-based contact methods, such as social media, websites, and apps. In 2019, 25% of consumers who reported an incident of international fraud initiating outside of the U.S. reported that they were first contacted via email. By June 30, 2023, only about half that many (12%) reported being contacted by email. Similarly, consumers have reported a drop from 17% to 8% in scammers initially contacting them by phone. Conversely, consumers have reported that contact through social media, websites or apps by scammers located outside of the U.S. has increased from 29% in 2019 to 53% by June 30, 2023. *Figure 8* shows annual and 2023 year-to-date details for the initial contact and payment methods employed by companies outside of the U.S. between January 1, 2019, and June 30, 2023. Further information in this format, updated quarterly, is available through the "Contact and Payment Method" tab located at https://public.tableau.com/app/profile/federal.trade.commission/viz/InternationalReports/TopCountries.

Figure 8: Fraud Reports Against non-U.S. Companies



Additional details on recent trends concerning contact and payment methods for fraud originating in Canada, China, India, Mexico, and the U.K. – the top five country locations reported by consumers in the U.S. since January 1, 2019 – is provided in *Figures 9* to *14*. (In these international trends, China and Hong Kong are reported separately; data for Macau is not available.) Among other things, this data shows:

- Consumers often pay scammers in Canada through wire transfer.
- Paying fraudsters in the U.K. and Hong Kong through cryptocurrencies has been common in recent years.
- Consumers who report fraud concerning China (excluding Hong Kong and Macau) are often contacted via social media or websites, and often pay with credit cards or debit cards.

Further information on these and other countries and regions, updated quarterly, is available by selecting specific countries or regions through the "Contact & Payment Method" tab located at https://public.tableau.com/app/profile/federal.trade.commission/viz/InternationalReports/TopCountries.

Figure 9: Fraud Reports Against Companies Located in Canada

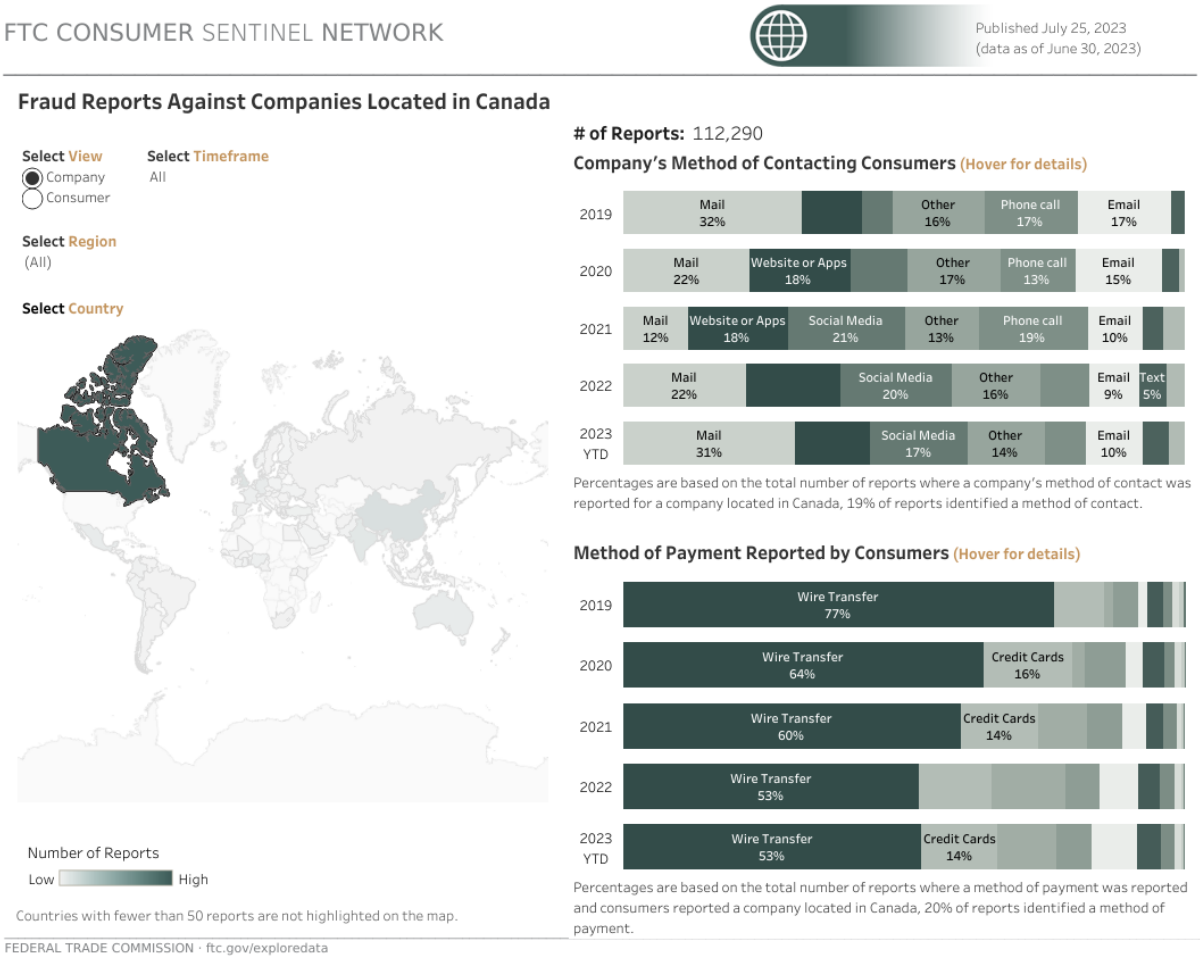


Figure 10: Fraud Reports Against Companies Located in China

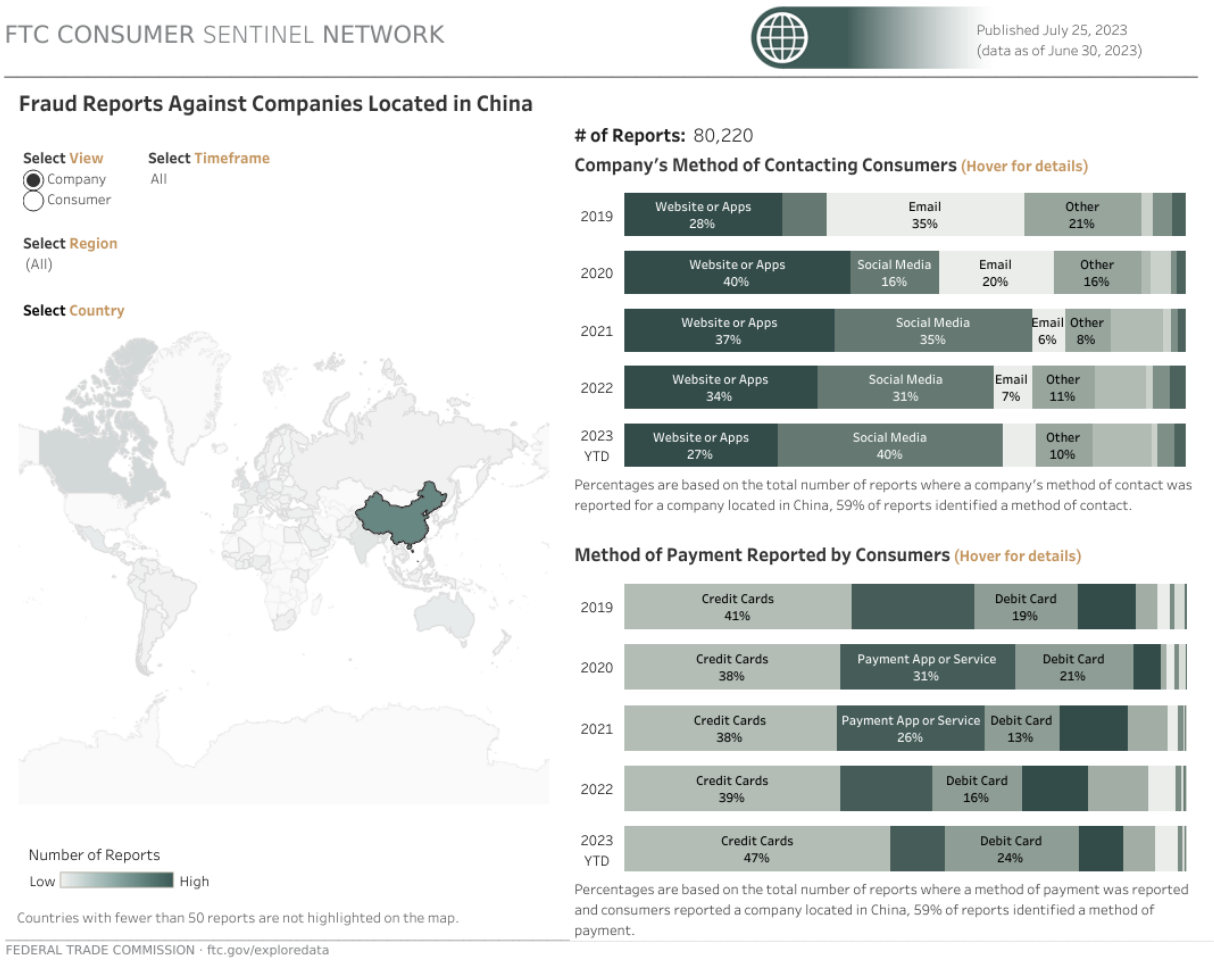


Figure 11: Fraud Reports Against Companies Located in Hong Kong

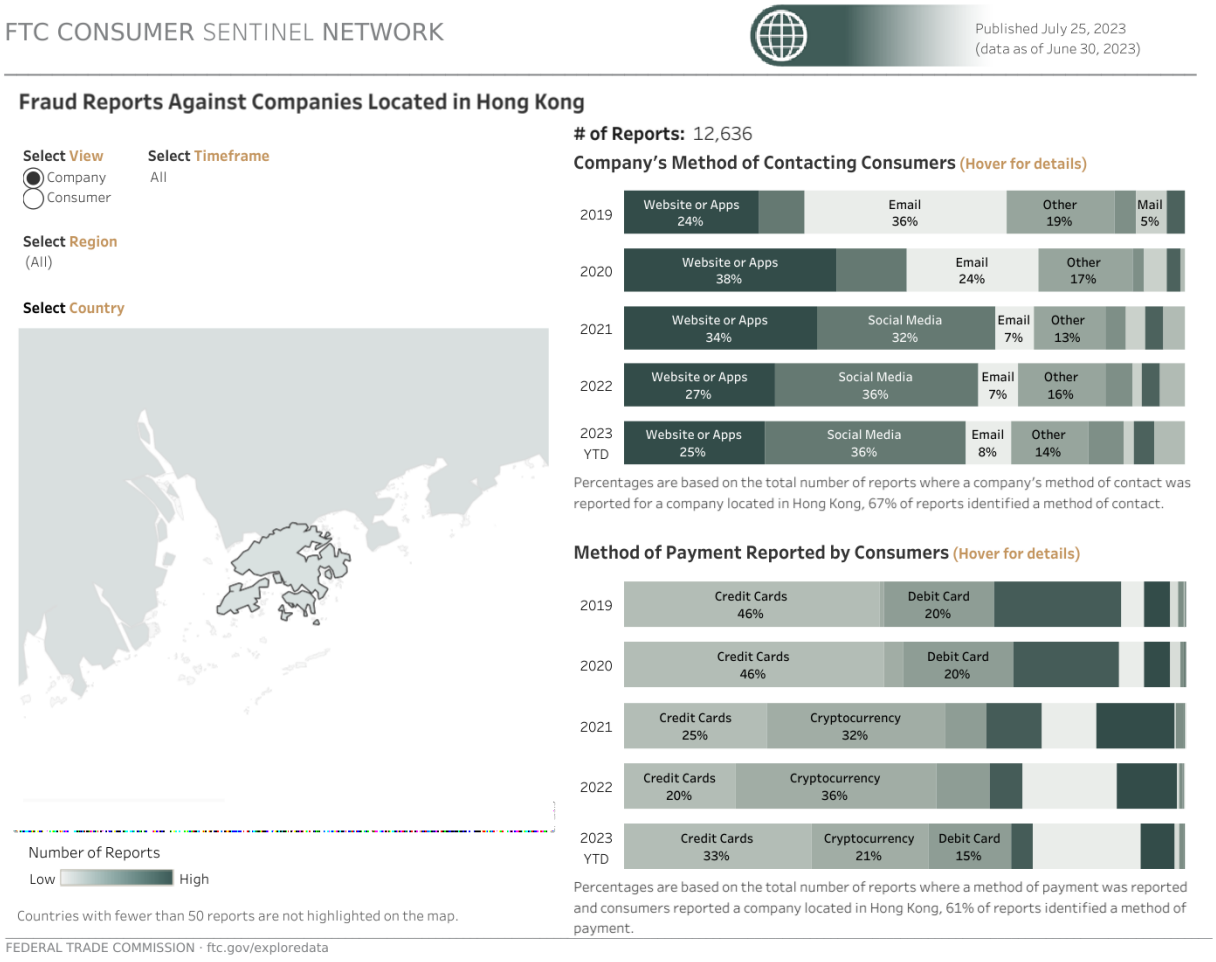


Figure 12: Fraud Reports Against Companies Located in India

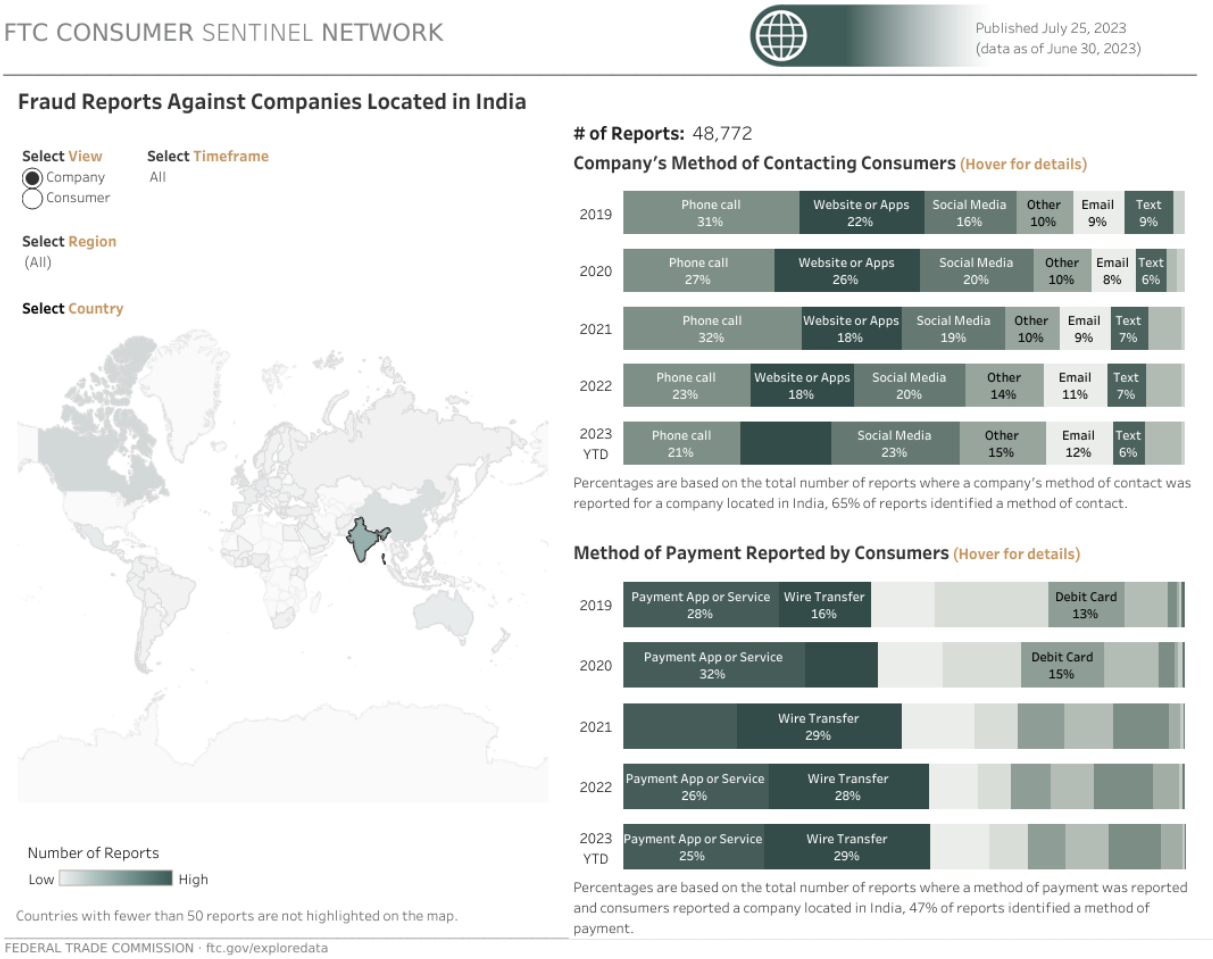


Figure 13: Fraud Reports Against Companies Located in Mexico

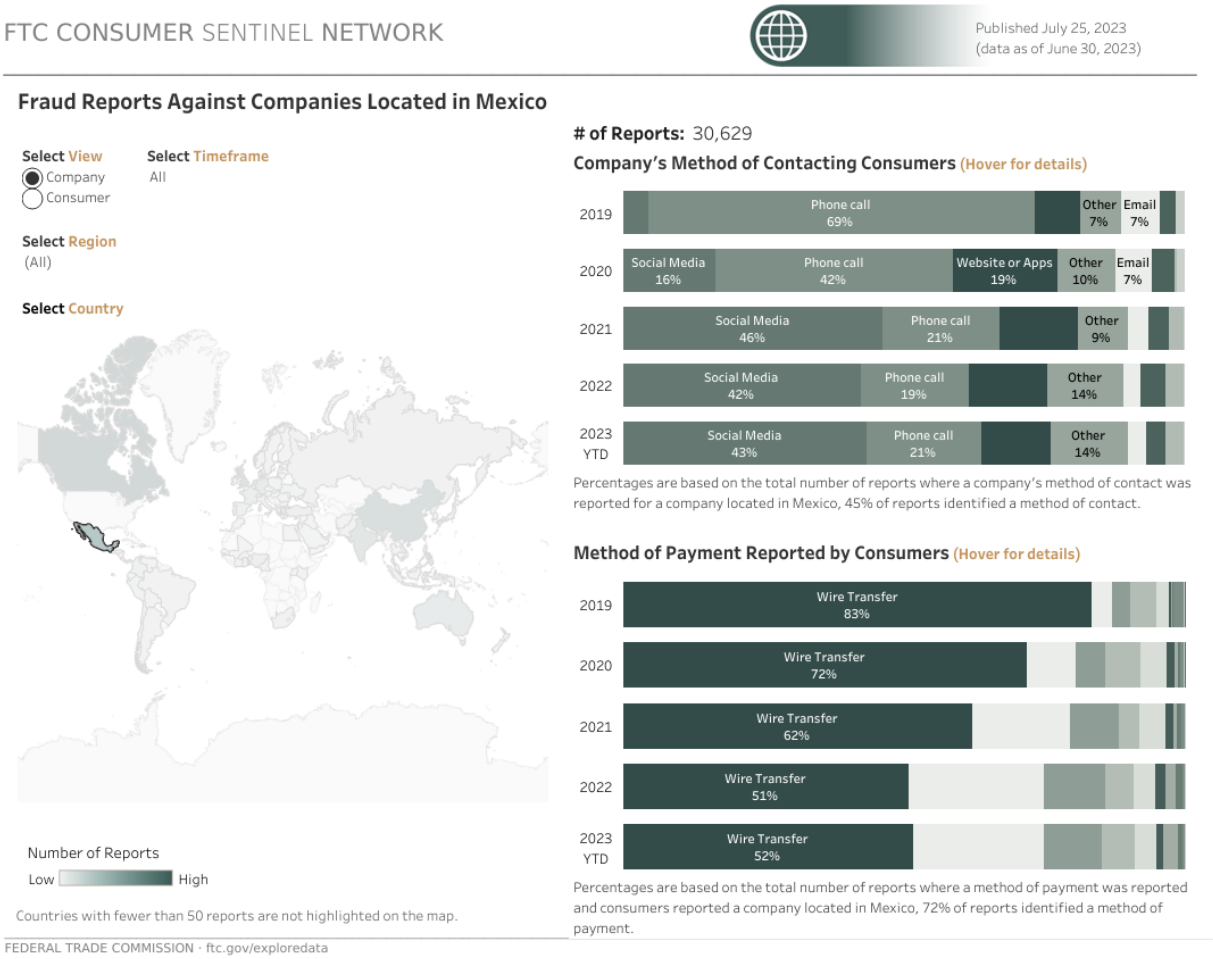
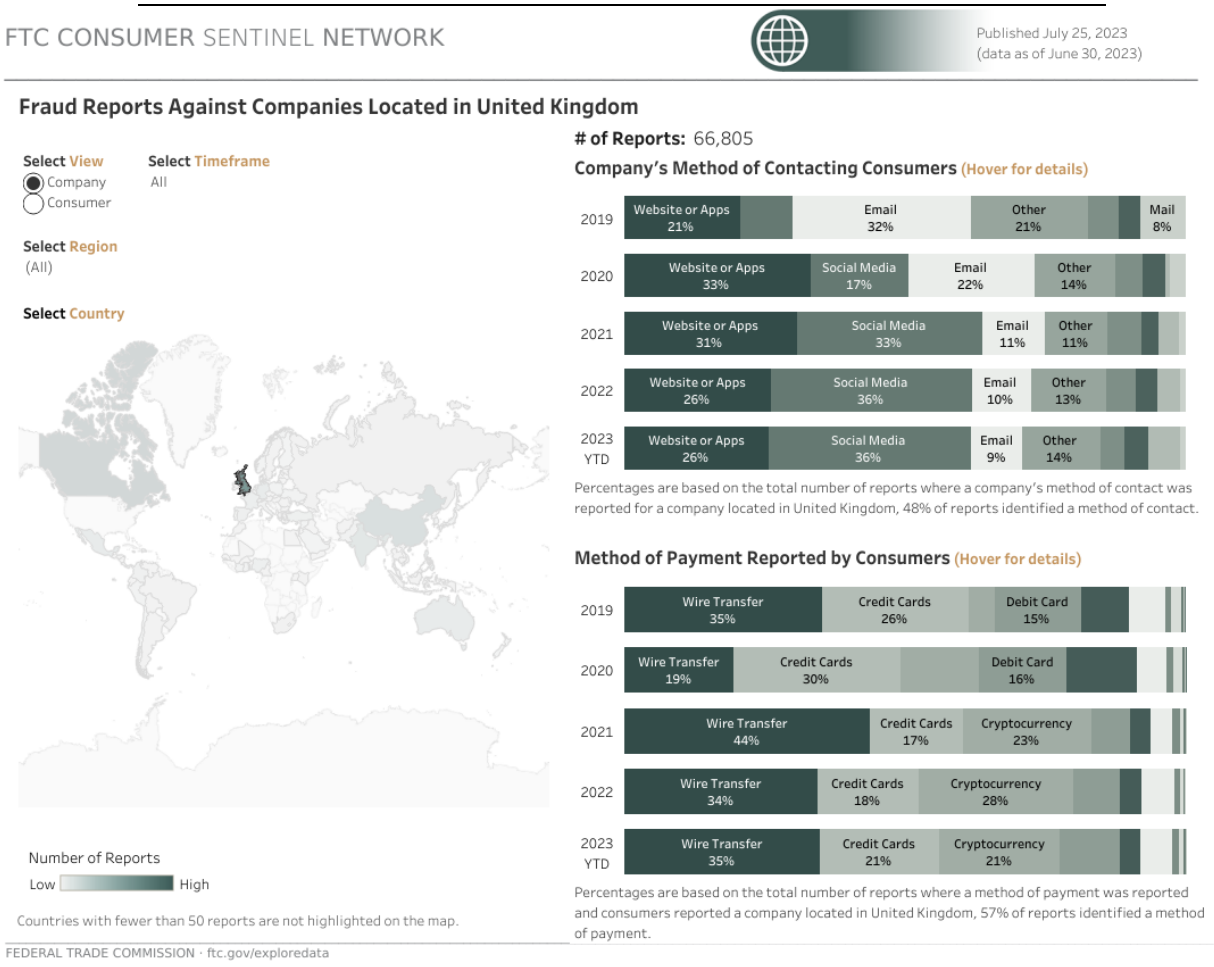


Figure 14: Fraud Reports Against Companies Located in the United Kingdom



Appendix B

Consumer Sentinel and Tableau Public

Consumer complaints, including cross-border complaints, are essential to the FTC's enforcement efforts, providing direct information about fraud and other harms that consumers encounter in the marketplace. The FTC and its law enforcement partners – through the ***Consumer Sentinel*** system – use and share complaints in a secure and confidential manner to identify enforcement targets and, with appropriate safeguards, as evidence in enforcement proceedings. The FTC also uses aggregate complaint data—through the ***Tableau Public*** system—to report publicly on complaint and fraud trends. The FTC does not act upon individual complaints.

Consumer Sentinel

Because complaints are so critical to the enforcement efforts of the FTC and its partners, the Commission has worked diligently for many years to first create and then expand the number of agencies and organizations, both foreign and domestic, that contribute data to or access ***Consumer Sentinel***. When Sentinel was launched in 1997, it was the first bi-national web-based fraud database to track consumer complaints in multiple jurisdictions. Since then, it has expanded into a robust multi-national, multi-state, multi-organization database that receives millions of complaints each year from **45** data contributors (*see* https://www.ftc.gov/enforcement/consumer-sentinel-network/data-contributors); an additional **29** entities also refer consumers to Consumer Sentinel to file complaints. In addition, over **1,000** law enforcement agencies are registered Sentinel members, including **44** foreign law enforcement agencies, with the FTC providing Sentinel access to **nearly 3,000** individual law enforcement professionals, with hundreds accessing the system weekly. As a result of ongoing improvements to Sentinel, these users can securely search, sort and view complaint data tailored to their needs while protecting consumer privacy.

How the FTC Receives Complaints

The FTC receives fraud complaints from consumers in both English and various other languages via its web-based complaint portal ReportFraud.ftc.gov and phone calls to the FTC's Consumer Response Center. Consumers can also report identity theft at IdentityTheft.gov and unwanted calls to the National Do Not Call Registry at donotcall.gov. This data is retained in the FTC's Consumer Sentinel database, a secure online database available only to registered law enforcement agencies and users. (A current list of member agencies can be found at https://register.consumersentinel.gov/Agency.)

In addition to reports received directly from consumers, Consumer Sentinel includes reports filed with **46** other federal, state, local, and foreign law enforcement agencies, as well as various private organizations. (Data contributors that are not enforcement agencies do not have access to the Sentinel database.) These contributions greatly improve the quantity and quality of information available to law enforcement about fraud and other consumer harms, including cross-border frauds. Important sources of cross-border fraud complaints include foreign law enforcement agencies, which are the Canadian

Competition Bureau, which has contributed to Sentinel for over two decades, and the Australian Competition and Consumer Commission, which became a data contributor in 2021. Combined, contributions from foreign law enforcement agencies, which are supported by SAFE WEB (*see* 15 U.S.C. § 57b-2(f) (concerning confidentiality, exemption from public disclosure, and material obtained from a foreign source)) accounted for 7% of all fraud complaints in Sentinel in 2021 and 2022. Another important source is econsumer.gov, a project started in 2001 by members of ICPEN. Through the econsumer.gov website, consumers can file cross-border reports and learn other steps to take to combat fraud, now in **nine** languages. Econsumer.gov receives tens of thousands of complaints each year.

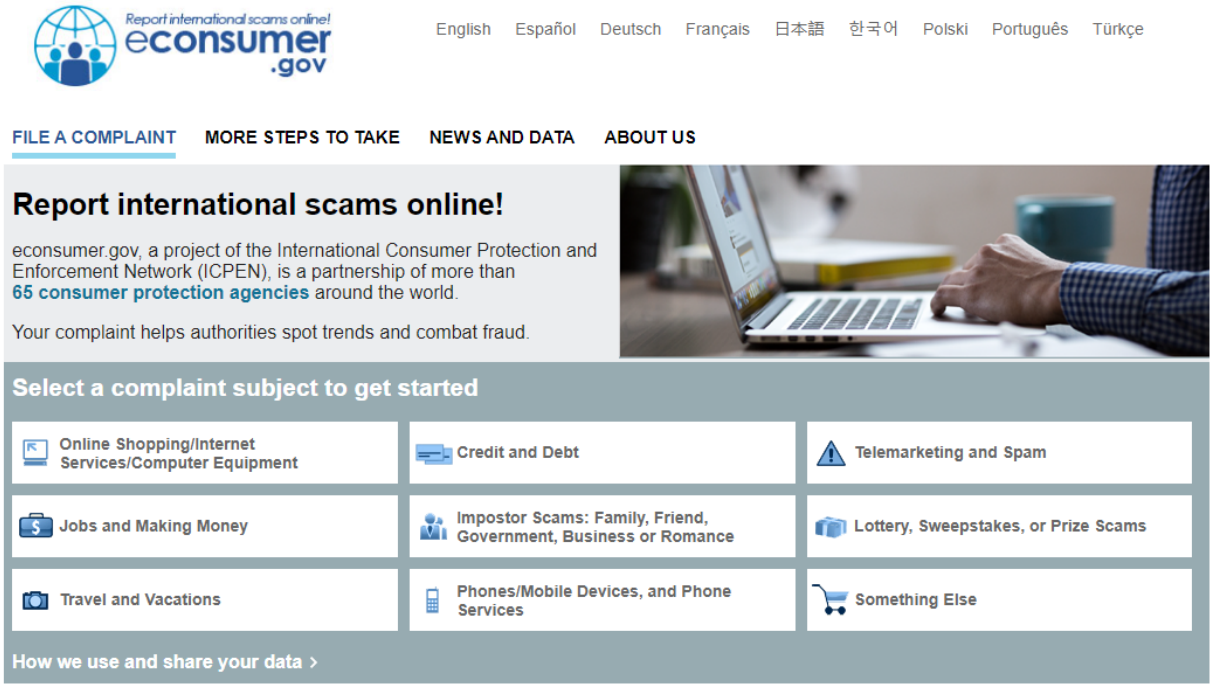


Photo 2 (econsumer.gov homepage showing where consumers can report international scams online.)

How the FTC Uses Complaints

The FTC uses consumer complaints to identify questionable business practices and targets and as evidentiary support and leads in its enforcement actions. Consumer complaints often describe the harmful practices or conduct consumers experience and provide essential investigation details such as business locations, websites, URLs, or apps. In addition, when the FTC needs to move quickly to stop an ongoing fraud, consumer complaints can provide critical evidence of the unfair or deceptive conduct and the extent of consumer harm. And when defendants lack the information necessary to provide consumer redress, complaints sometimes help to identify injured consumers.

The FTC also uses and acts on consumer complaints by sharing them in a secure, confidential manner with qualified law enforcement partners through Sentinel, which helps to make law enforcement more cooperative and effective. In addition to numerous domestic agencies, several Canadian and Australian agencies can access consumer complaints through Sentinel. The FTC has also worked through ICPEN to

expand foreign law enforcement access to cross-border complaints, including through econsumer.gov, and ICPEN members that have agreed to confidentiality and data security requirements can access econsumer.gov complaints through Sentinel. Combined, **44** foreign law enforcement agencies are registered Sentinel users.

Tableau Public Page

In addition to providing confidential access to complaints, as described above, and sharing complaints through SAFE WEB, the FTC also analyzes consumer complaints to identify and make public aggregate trend data. For example, consumer complaints housed in Sentinel can be analyzed by various attributes, including **100** fraud and other subcategories (such as online shopping and imposter scams), as well as business location, consumers location, complaint source, contact and payment methods, and more.

For over two decades, the FTC has publicly reported on aggregate complaint trends through its Consumer Sentinel Network Reports (*see* https://www.ftc.gov/enforcement/consumer-sentinel-network/reports) and Annual Reports (*see* https://www.ftc.gov/policy/reports/ftc-annual-reports). In 2018, as part of its ongoing efforts to improve on its ability to analyze, report on, and share aggregate public information about consumer complaints, the FTC launched its interactive Tableau Public page (available at https://public.tableau.com/app/profile/federal.trade.commission/viz/federal.trade.commission#!/).

Through the FTC's ***Tableau Public*** page, members of the public can view up to five years of annual and quarterly complaint data through multiple interactive visualizations. This includes data on international complaints. Thus, for example, through the FTC's International Reports visualizations, the public can see fraud reports against the top 50 non-U.S. locations through a table and an interactive map where, by simply clicking on a country, responsive data for that country appears. (*See Figures 15 and 16*.) The public can also find data visualizations about the most common contact methods and payment methods used when consumers interact with non-U.S. companies (*see* Appendix A) and summaries of complaints to the econsumer.gov website.

Figure 15: Fraud Reports Against Top 50 non-U.S. Company Locations

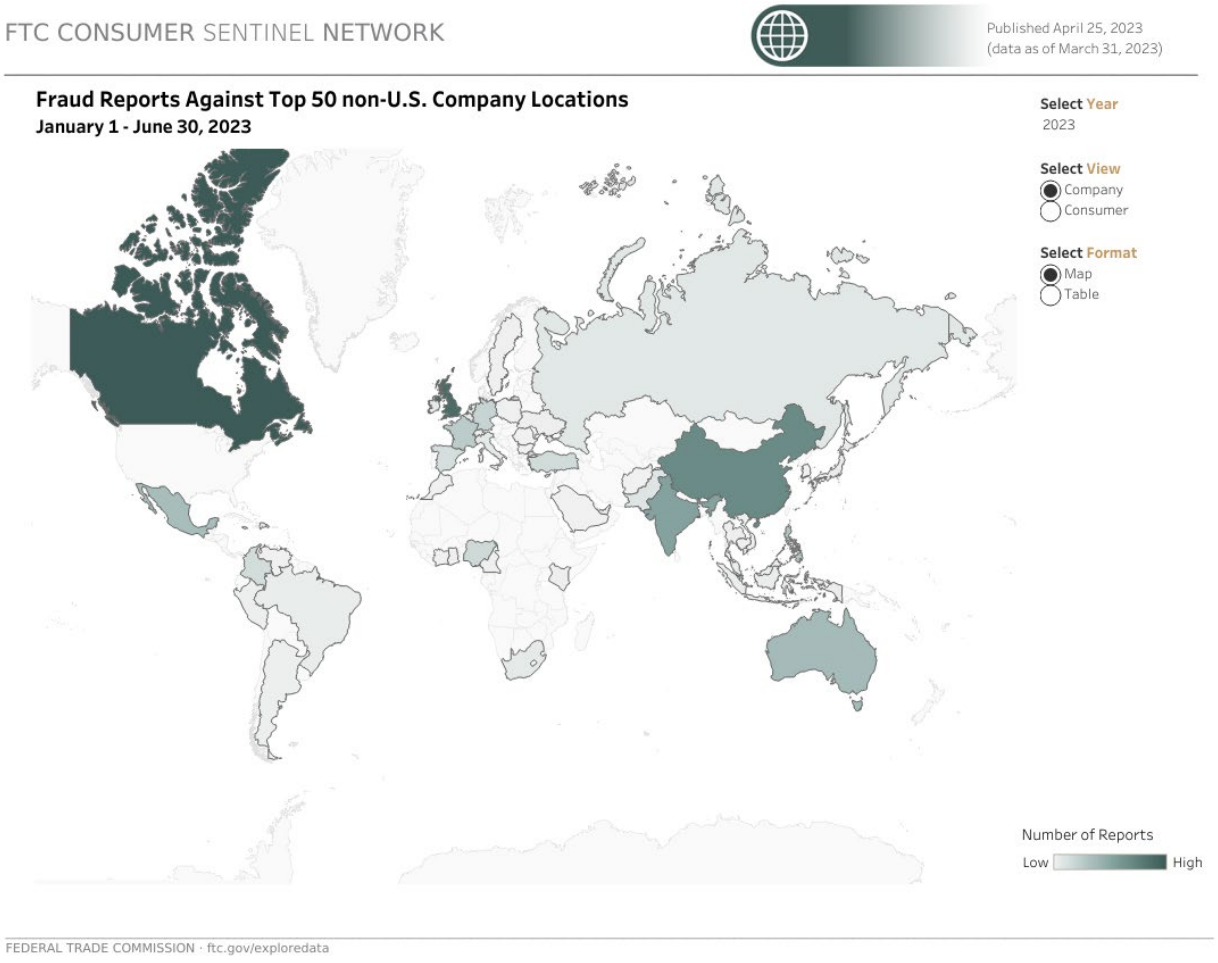


Figure 16: Fraud Reports Against Top 50 non-U.S. Company Locations

FTC CONSUMER SENTINEL NETWORK

Published April 25, 2023
(data as of March 31, 2023)

Fraud Reports Against Top 50 non-U.S. Company Locations

January 1 - June 30, 2023

Select Year
2023

Select View
(•) Company
( ) Consumer

Select Format
( ) Map
(•) Table

		# of Reports
1	CANADA	3,927
2	UNITED KINGDOM	3,494
3	CHINA	2,721
4	INDIA	2,128
5	AUSTRALIA	1,482
6	MEXICO	1,416
7	PHILIPPINES	1,229
8	FRANCE	1,041
9	GERMANY	837
10	NIGERIA	698
11	TURKEY	650
12	COLOMBIA	623
13	HONG KONG	599
14	SPAIN	572
15	PAKISTAN	407
16	DOMINICAN REPUBLIC	397
17	RUSSIA	347
18	SINGAPORE	306
19	UNITED ARAB EMIRATES	292
20	ITALY	290
21	SOUTH AFRICA	288
22	IRELAND	280
23	NETHERLANDS	269
24	JAMAICA	260
25	BELGIUM	239

		# of Reports
26	BRAZIL	222
27	SWITZERLAND	200
28	JAPAN	199
	MALAYSIA	199
30	INDONESIA	193
31	PERU	166
32	ARGENTINA	164
33	KENYA	161
34	UKRAINE	158
35	THAILAND	150
36	CAMEROON	146
37	CAMBODIA	145
38	POLAND	143
39	VIET NAM	136
40	SWEDEN	125
41	GHANA	124
42	CYPRUS	116
43	MOROCCO	113
44	ROMANIA	111
45	VENEZUELA	109
46	COTE D'IVOIRE	107
	SAUDI ARABIA	107
48	SOUTH KOREA	101
49	AFGHANISTAN	100
50	BULGARIA	96

FEDERAL TRADE COMMISSION · ftc.gov/exploredata

Appendix C

FTC Enforcement Actions with Public Cross-Border Components

(Cases filed between January 1, 2007, and June 30, 2023)

This list includes cases filed in which public information indicates that one or more of the defendants is located abroad or there is some other significant foreign component, such as key foreign witnesses or other important evidence located abroad, 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 disclosed publicly.

	Case Caption	Noteworthy Conduct and Relief	Cross-Border Component(s)	Initial Press Release	Redress and Other Notable Activities
Through June 30, 2022					
1	*U.S. v. Nexway SASU*, No. 1:23-cv-900 (D.D.C. Apr. 3, 2023)	Defendants, a multi-national payment processing company, its CEO, and chief strategy officer, are alleged to have facilitated tech support scammers through credit card laundering, going back to at least 2016.	Defendant Nexway SASU is a French corporation which became part of defendant Nexway Group AG, a Swiss corporation in 2018. Defendant asknet Solutions AG is a German corporation.	FTC Acts to Block Payment Processor's Credit Card Laundering for Tech Support Scammers	
2	*U.S. v. Stratics Networks, Inc.*, No. 3:23-cv-00313-BAS-KSC (S.D. Cal. Feb. 16, 2023)	Defendants, an outbound calling service, are alleged to have assisted and facilitated violations of the Telemarketing Sales Rule ("TSR") by enabling its clients to route and transmit millions of	Defendant Stratics Networks is a Canadian corporation.	FTC Sues to Stop Interconnected Web of VoIP Service Providers Carrying Robocalls Pitching Phony Debt Relief Services	

		robocalls using VoIP technology.			
3	*FTC v. WealthPress, Inc.*, No. 3:23-cv-00046 (M.D. Fl. Jan. 12, 2023)	Defendants, an investment advice company and its owners, were alleged to have made deceptive claims to sell consumers investment advising services that cost consumers hundreds or thousands of dollars. A settlement order requires defendants to refund more than $1.2 million to consumers and pay a $500,000 civil penalty for deceiving consumers with false claims about their services.	Defendant Conor Lynch owned one third of Wealth Press through a Canadian based company Happy Camper Publishing, Inc.	FTC Suit Requires Investment Advice Company WealthPress to Pay $1.7 Million for Deceiving Consumers	
2022					
4	*In the Matter of Electrowarmth Prods., LLC*, File No. 222-3096, Docket No. C-4779 (Aug. 30, 2022)	Respondents were alleged to have deceptively claimed that products were "made in the USA" when they were made in China. Settlement prohibits respondents from making misleading or unsubstantiated country of origin claims.	Respondent Electrowarmth's heated fabric mattress pad products were wholly manufactured, labeled, and packaged in China.	FTC Sues Heated Mattress Pads Marketer Electrowarmth for Falsely Claiming that Chinese Products Were Made in the USA	Final Order (Oct. 28, 2022)

5	*FTC v. Walmart Inc.*, No. 1:22-cv-3372 (N.D. Ill. June 28, 2022)	Defendant alleged to have injured consumers by failing to take timely, appropriate, and effective action to detect and prevent fraud-induced money transfers, and to have assisted and facilitated violations of the TSR through the processing of money transfers.	Walmart transacted business throughout the United States and in other countries worldwide, including by offering and facilitating money transfer services around the world.	FTC Sues Walmart for Facilitating Money Transfer Fraud That Fleeced Customers Out of Hundreds of Millions	
6	*FTC v. Warrior Trading Inc.*, No. 3:22-cv-30048 (D. Mass. Apr. 19, 2022)	Defendants, an alleged day-trading investment scheme, made misleading and unrealistic claims of big investment gains to consumers who paid hundreds or thousands of dollars for a system that ultimately failed to pay off for most customers. As a result of a settlement, Warrior Trading was required to pay $3 million to refund consumers and was prohibited from making baseless claims about the potential for consumers to earn money using their trading strategies.	Defendants advertised, marketed, promoted, and sold their day-trading strategies and related goods and services to consumers throughout the United States and internationally.	Federal Trade Commission Cracks Down on Warrior Trading for Misleading Consumers With False Investment Promises	FTC Returns More Than $2.9 Million To Consumers Harmed by Warrior Trading (Jan. 10, 2023)

7	*FTC v. Hum. Res. Dev. Servs., Inc., also d/b/a Saint James Sch. of Med.*, No. 1:22-cv-1919, (N.D. Ill. Apr. 14, 2022)	Defendants alleged to have deceptively marketed their school's medical license exam test pass rate and residency matches to lure prospective students. Defendants also alleged to have violated the Holder Rule, which preserves rights for injured consumers, and the Credit Practices Rule, which protects consumers in credit contracts. Settlement bans defendants from misrepresenting medical license test pass rates, residency matches, and making unsubstantiated claims, and ordered them to pay $1.2 million in redress.	Saint James School of Medicine is a for-profit medical school in the Caribbean.	Federal Trade Commission Takes Action Against For-Profit Medical School for Using Deceptive Marketing to Lure Students	Federal Trade Commission Returns More Than $830,000 to Students Misled by Saint James Medical School's Deceptive Marketing Claims (Nov. 3, 2022)
8	*U.S. v. Turbo Sols. Inc., f/k/a Alex Miller Fin. Serv.*, No. 4:22-mc-369 (S.D. Tex. Mar. 1, 2022)	Defendants alleged to have defrauded consumers out of millions of dollars by falsely claiming they would remove negative information from credit reports in exchange for a fee. Defendants also alleged to have filed fake identity theft reports to explain negative items on	Turbo Solutions employees or contractors operated from the Philippines.	FTC Halts Deceptive Credit Repair Operation that Filed Fake Identity Theft Complaints	

		customers' credit reports.			
9	*In the Matter of Fashion Nova, Inc.*, File No. 192-3138, Docket No. C-4759 (Jan. 25, 2022)	Respondent, an online fashion retailer, was alleged to have engaged in deceptive review practices by only publishing four- and five-star customer reviews of products and by suppressing thousands of lower starred, negative reviews. Settlement required respondent to pay $4.2 million for the harm it caused consumers.	Fashion Nova transacted business throughout the United States and in other countries worldwide.	Fashion Nova will Pay $4.2 Million as part of Settlement of FTC Allegations it Blocked Negative Reviews of Products	Final Order (March 18, 2022) FTC Announces Refund Claims Process for Fashion Nova Customers Affected by Deceptive Review Practices (May 17, 2023)
2021					
10	*U.S. v. Kuuhuub Inc.*, No. 1:21-cv-01758 (D.D.C. July 1, 2021) (a/k/a Recolor Oy)	Defendants, operators of an online coloring book app, were alleged to have violated the Children's Online Privacy Protection Act (COPPA) Rule by collecting and disclosing personal information about children who used the app without notifying their parents and obtaining consent. Settlement required defendants to notify	Defendant Kuuhuub Inc. is a Canadian corporation. Defendants Kuu Hubb Oy and Recolor Oy are Finnish subsidiaries of Kuuhuub Inc.	Online Coloring Book App Recolor Settles FTC Allegations It Illegally Collected Kids' Personal Information	

		parents and offer refunds for underage subscribers.			
11	*In the Matter of BASF SE*, File No. 192-3088, Docket No. C-4744, C-4745 (Apr. 1, 2021).	Respondents alleged to have deceptively marketed fish oil supplements as clinically proven to reduce liver fat in adults and children with non-alcoholic fatty liver disease. Settlements ban the companies from making unproven health claims and require them to pay over $416,000 – enough money to provide full refunds to over 1,800 consumers nationwide.	BASF SE is multi-national corporation based in Germany.	Companies Settle FTC Charges that They Deceptively Marketed Fish Oil Supplements with False Claims They Were Clinically Proven to Treat Liver Disease	Final Order as to BASF SE and BASF Corp. (June 1, 2021) Final Order as to DIEM Labs, LLC and related individuals (June 1, 2021) FTC Sends Full Refunds to Consumers who Bought Deceptively Marketed Fish Oil Supplement (Feb. 8, 2022)
12	*In the Matter of Residual Pumpkin Entity, LLC, formerly d/b/a CafePress*, File No. 192-3209, Docket Nos. C-4768, C-4769 (Mar. 15, 2021)	Respondents alleged to have failed to implement reasonable security measures to protect sensitive information stored on CafePress's network and to have covered up a major breach that included plain text Social Security numbers, inadequately encrypted passwords, and answers to password reset questions. Respondents also alleged	Respondents misrepresented their adherence to the EU-U.S. and Swiss-U.S. Privacy Shield frameworks and misrepresented that they would honor requests from residents of the EU and Switzerland to erase and restrict the use of personal data.	FTC Takes Action Against CafePress for Data Breach Cover Up	Final Order (June 23, 2022)

		to have misrepresented their adherence to the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield frameworks. Settlement ordered respondents to implement comprehensive information security programs and Respondent Residual Pumpkin (CafePress) ordered to pay $500,000 to victims of data breach.			
13	*In the Matter of Flo Health, Inc.*, File No. 192-3133, Docket No. C-4747 (Jan. 13, 2021)	Respondent, the developer of a popular fertility tracking app, allegedly promised to keep users' health data private and only use it for app services, but instead disclosed it to third parties that provided marketing and analytics services. Respondent also alleged to have violated the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield frameworks. Settlement required the respondent to obtain the affirmative consent of its users before sharing their	Data transfers under the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield frameworks. Respondent's Flo app was downloaded by more than 19 million users in the EU and Switzerland.	Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data	Final Order (June 17, 2021)

		personal health information and to obtain an independent review of its privacy practices.			
2020					
14	*In the Matter of Ascension Data & Analytics, LLC*, File No. 192-3126, Docket No. C-4758 (Dec. 15, 2020)	Respondents, a mortgage industry data analytics company, allegedly failed to ensure that one of its vendors, which was hired to perform text recognition scanning, was adequately securing personal data about tens of thousands of mortgage holders in violation of the Gramm-Leach Bliley Act's Safeguards Rule. The cloud-based server that stored the data in plain text and without other protections was accessed roughly 52 times by unauthorized IP addresses, including from Russia and China. The settlement requires the company to bolster its data security protections and oversight of its vendors to ensure third-party providers are also	Unauthorized IP addresses from Russia and China accessed a cloud-based server that stored personal data on tens of thousands of consumers in plain text and without other protections	Mortgage Analytics Company Settles FTC Allegations It Failed to Ensure Vendor Was Adequately Protecting Consumer Data	Final Order (Dec. 22, 2021)

		complying with those safeguards.			
15	*In the Matter of Miniclip S.A.*, File No. 192-3129, Docket No. C-4722 (May 19, 2020)	Respondent, a digital game developer, was alleged to have falsely claimed, from 2015 through mid-2019, that it was a member of the Children's Advertising Review Unit's (CARU) COPPA safe harbor program despite its membership having been terminated in 2015. Miniclip is prohibited from misrepresenting its participation or certification in any privacy or security program sponsored by a government or any self-regulatory organization, including the CARU COPPA safe harbor program	Respondent Miniclip is a Swiss corporation.	Swiss Digital Game Developer Settles FTC Allegations that it Falsely Claimed it was a Member of COPPA Safe Harbor Program	Final Order (June 29, 2020)
16	*FTC v. Fashion Nova, Inc.*, No. 2:20-cv-3641 (C.D. Cal. Apr. 20, 2020)	Defendant, an online fashion retailer, was alleged to have failed to notify consumers and give them the opportunity to cancel their orders when the company did not ship ordered merchandise in a	Fashion Nova marketed and sold merchandise to consumers throughout the United States and in many other countries. Consumers in over fifty countries complained about Fashion Nova's	Fashion Nova Will Pay $9.3 Million for Consumer Refunds To Settle FTC Charges It Violated Rules On Shipping, Refunds	FTC Sends More Than $6.5 Million to Consumers Harmed by Fashion Nova (Mar. 25, 2021)

		timely manner. Defendant were also alleged to have illegally issued gift cards to compensate consumers for unshipped merchandise instead of providing refunds. As part of a settlement, the defendant was ordered to pay $9.3 million.	practices and the FTC provided redress to consumers in 169 different countries.		
17	*FTC v. Bransfield*, No. 6:20-cv-00372 (M.D. Fla. Mar. 3, 2020)	Defendants, affiliate marketers for the business coaching and investment scheme known as "My Online Business Education" (MOBE), were alleged to have helped deceive consumers by making false and misleading earnings claims. Settlement orders permanently ban defendants from selling or marketing any business coaching program or money-making method. Defendant John Chow and his company TTZ Media were ordered to pay $3.35 million for consumer redress.	Defendant TTZ Media is a Canadian corporation.	Affiliate Marketers to Pay More Than $4 Million to Settle Charges that They Promoted a Fraudulent Business Coaching and Investment Scheme	

18	*FTC v. OTA Franchise Corp.*, No. 8:20-cv-00287-JVS (C.D. Cal. Feb. 12, 2020)	Defendants alleged to have deceived consumers with false and unsubstantiated claims that purchasers of the Online Trading Academy's (OTA) investment training were likely to earn significant income. Defendants also alleged to have illegally used form contracts to prevent consumers from complaining to the government or others about OTA's deception. Defendants were ordered, as part of a settlement, to forgive $13.3 million in debt owed by consumers.	Defendants advertised, marketed, distributed, promoted, and sold their training programs to consumers throughout the United States and internationally, and operated training centers in Vancouver, Canada and London, England.	FTC Sues Online Trading Academy for Running an Investment Training Scheme	Federal Trade Commission Sending Refunds to More than 31,000 Consumers Allegedly Defrauded by Online Training Academy (Aug. 16, 2021)
19	*FTC v. Noland*, No. CV-20-0047-PHX-DWL (D. Ariz. Jan. 21, 2020) (complaint amended Sep. 24, 2020) (a/k/a Success by Health)	Defendants operated "instant coffee" and travel pyramid schemes that used false promises of wealth and income to entice thousands of consumers to join. After a trial, the court imposed a $7.3 million monetary judgment on defendants, and permanently banned defendants from any	The FTC presented evidence of defendant Noland's efforts to move assets abroad and relocate to Uruguay. In granting the FTC's preliminary injunction, the court found that defendant Noland used corporate funds to pay for homes in the United States and Uruguay.	FTC Acts to Shut Down 'Success by Health' Instant Coffee Pyramid Scheme	Order (May 11, 2023) Federal Court Finds James D. 'Jay' Noland, Jr., Operator of 'Success By Health' and 'VOZ Travel,' in Contempt of Court Order Barring Pyramid Schemes (May 25, 2023)

		participation in multi-level marketing.			
2019					
20	*FTC v. On Point Glob. LLC*, No.1:19-cv-25046-RNS (S.D. Fla. Dec. 12, 2019)	Defendants deceptively operated hundreds of fake government websites that promised quick and easy services, such as renewing a driver's license, but instead provided only publicly available, general information about the sought service. The FTC's trial win against On Point Global made $102 million in refunds available to consumers who were harmed by defendants.	Defendants owned subsidiaries and ran a web development office and call centers in Costa Rica and Uruguay. Defendants also established holding companies in Nevis (part of Saint Kitts and Nevis), Belize, and the Bahamas to shelter the proceeds of the fraud.	Court Stops Sprawling Scheme That Operated Hundreds of Websites That Deceived Consumers About Government Services	FTC Win at Trial Against On Point Global Makes $102 Million in Refunds Available for Consumers Harmed by Fake Government Website Scams (Apr. 7, 2022)
21	*In the Matter of NTT Global Data Centers Americas, Inc., as successor in interest to RagingWire Data Centers, Inc.*, File No. 182-3189, Docket No. 9386 (Nov. 7, 2019)	Respondent alleged to have misled consumers about its participation in the EU-U.S. Privacy Shield framework and failed to adhere to the program's requirements before allowing its certification to lapse. Under a settlement, the company is prohibited from misrepresenting its	Data transfers under the EU-U.S. Privacy Shield framework.	FTC Charges Nevada Company with Falsely Claiming Participation in the EU-U.S. Privacy Shield	Final Order (Oct. 28, 2020)

		compliance with or participation in the Privacy Shield framework, and any other privacy or data security program sponsored by the government or any self-regulatory or standard-setting organization.			
22	*In the Matter of DCR Workplace, Inc.*, File No. 182-3188, Docket No. C-4698 (Sept. 3, 2019)	Respondent alleged to have falsely claimed certification under the EU-U.S. Privacy Shield framework. Under the terms of a settlement, the company is prohibited from misrepresenting its participation in the EU-U.S. Privacy Shield framework, any other privacy or data security program sponsored by the government, or any self-regulatory or standard-setting organization.	Data transfers under the EU-U.S. Privacy Shield framework.	Five Companies Settle FTC Allegations that they Falsely Claimed Participation in the EU-U.S. Privacy Shield	
23	*In the Matter of 214 Techs., Inc., also d/b/a Trueface.ai*, File No. 182-3193, Docket No. C-4699 (Sept. 3, 2019)	Respondent alleged to have falsely claimed certification under the EU-U.S. Privacy Shield framework.	Data transfers under the EU-U.S. Privacy Shield framework.	Five Companies Settle FTC Allegations that they Falsely Claimed Participation in the EU-U.S. Privacy Shield	

		Under the terms of a settlement, the company is prohibited from misrepresenting its participation in the EU-U.S. Privacy Shield framework, any other privacy or data security program sponsored by the government, or any self-regulatory or standard-setting organization.			
24	*In the Matter of LotaData, Inc.*, File No. 182-3194, Docket No. C-4700 (Sept. 3, 2019)	Respondent alleged to have falsely claimed certification under the EU-U.S. and Swiss-U.S. Privacy Shield framework. Under the terms of a settlement, the company is prohibited from misrepresenting its participation in the EU-U.S. Privacy Shield framework, any other privacy or data security program sponsored by the government, or any self-regulatory or standard-setting organization.	Data transfers under the EU-U.S. and Swiss-U.S. Privacy Shield framework.	Five Companies Settle FTC Allegations that they Falsely Claimed Participation in the EU-U.S. Privacy Shield	

25	*In the Matter of EmpiriStat, Inc.*, File No. 182-3195, Docket No. C-4701 (Sept. 3, 2019)	Respondent, among other things, was alleged to have falsely claimed that it was a current participant in Privacy Shield after allowing its certification to lapse. Under the terms of a settlement, the company is prohibited from misrepresenting its participation in the EU-U.S. Privacy Shield framework, any other privacy or data security program sponsored by the government, or any self-regulatory or standard-setting organization.	Data transfers under the EU-U.S. Privacy Shield framework.	Five Companies Settle FTC Allegations that they Falsely Claimed Participation in the EU-U.S. Privacy Shield	
26	*In the Matter of Thru, Inc.*, File No. 182-3196, Docket No. C-4702 (administrative complaint filed Sept. 3, 2019)	Respondent alleged to have falsely claimed certification under the EU-U.S. Privacy Shield framework. Under the terms of a settlement, the company is prohibited from misrepresenting its participation in the EU-U.S. Privacy Shield framework, any other privacy or data security program sponsored by the	Data transfers under the EU-U.S. Privacy Shield framework.	Five Companies Settle FTC Allegations that they Falsely Claimed Participation in the EU-U.S. Privacy Shield	

		government, or any self-regulatory or standard-setting organization.			
27	*In the Matter of Kogan*, File Nos. 182-3106 and 182-3107, Docket Nos. C-4693 and C-4694 (July 24, 2019)	Respondents, former Cambridge Analytica CEO Alexander Nix and app developer Aleksandr Kogan, were alleged to have employed deceptive tactics to harvest personal information from tens of millions of Facebook users for voter profiling and targeting. As part of a settlement, Kogan and Nix are prohibited from making false or deceptive statements regarding the extent to which they collect, use, share, or sell personal information, as well as the purposes for which they collect, use, share, or sell such information. In addition, they are required to delete or destroy any personal information collected from consumers via Kogan's GSRApp, which connects individuals to their Facebook profiles, and any related work product	Respondent Nix is a British citizen and was residing in the United Kingdom (U.K."). Respondent Kogan was the owner and co-founder of the now-defunct U.K. corporation, Global Science Research, Ltd. (GSR).	FTC Sues Cambridge Analytica, Settles with Former CEO and App Developer	Order as to Aleksandr Kogan (Dec. 18, 2019) Order as to Alexander Nix (Dec. 18, 2019)

		that originated from the data.			
28	*In the Matter of Cambridge Analytica, LLC*, File No. 182-3107, Docket No. 9383 (July 22, 2019)	Respondent, a data analytics company, was found by the FTC to have employed deceptive tactics to harvest personal information from tens of millions of Facebook users for voter profiling and targeting. Respondent also found by the FTC to have falsely claimed, until at least November 2018, that it was a participant in the EU-U.S. Privacy Shield framework, despite allowing its certification to lapse in May 2018. The FTC's Final Order prohibits the company from making misrepresentations about the extent to which it protects the privacy and confidentiality of personal information, as well as its participation in the EU-U.S. Privacy Shield framework and other similar regulatory or standard-setting organizations. The company is also required	Respondent company is part of a privately held U.K. corporation.	FTC Sues Cambridge Analytica, Settles with Former CEO and App Developer	Final Order and Opinion (Nov. 25, 2019) FTC Issues Opinion and Order Against Cambridge Analytica For Deceiving Consumers About the Collection of Facebook Data, Compliance with EU-U.S. Privacy Shield (Dec. 6, 2019)

		to continue to apply Privacy Shield protections to personal information it collected while participating in the program (or to provide other protections authorized by law) or return or delete the information. It also must delete the personal information that it collected through the GSRApp, which connects individuals to their Facebook profiles.			
29	*FTC v. Madera Merch. Servs., LLC*, No. 3:19-cv-00195-KC (W.D. Tex. July 19, 2019)	Defendants, Madera Merchant Services and B&P Enterprises, were alleged to have generated and processed remotely created payment orders (RCPOs) that allowed deceptive telemarketing schemes, including American Financial Benefits Center, Impetus Enterprise and Educare Centre Services, to withdraw money from their victims' bank accounts. Under terms of a settlement order,	Defendants processed payments for foreign enterprise Educare Centre Services, which was one of its largest clients and was based out of Canada and the Dominican Republic.	FTC and Ohio Stop Rogue Payment Processor and a Credit Card Interest-Reduction Telemarketing Scheme that Allegedly Worked Together to Scam Consumers	Rogue Payment Processor that Helped Perpetuate Multiple Scams Is Banned from the Payment Processing Business Under FTC Settlement (June 9, 2020)

		defendants were banned from payment processing.			
30	*FTC v. Educare Ctr. Servs., Inc.*, No. 3:19-cv-00196-KC (W.D. Tex. July 18, 2019)	Defendants alleged to have sold sham credit card interest rate reduction services to consumers and to have violated the TSR, including by failing to access to the FTC's Do Not Call Registry. Under the terms of settlement orders, defendants were prohibited from participating in any telemarketing in the United States and from marketing debt relief products or services of any kind.	Defendants Educare (a New Jersey company) and Prolink Vision (a Dominican Republic company) were alleged to have operated from Canada. Four Canadian citizens were also alleged to have managed and controlled the scheme from Canada. And a Canadian relief defendant received over $1 million from the scheme.	FTC and Ohio Stop Rogue Payment Processor and a Credit Card Interest-Reduction Telemarketing Scheme that Allegedly Worked Together to Scam Consumers	FTC Sends Nearly $2.3 Million in Refunds to People who Lost Money to Credit Card Debt Relief Schemes (July 29, 2021)
31	*In the Matter of SecurTest, Inc.*, File No. 182-3152, Docket No. C-4685 (June 14, 2019)	Respondent, which offered background screening services, was alleged to have falsely claimed that it complied with the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield frameworks. A settlement with the company prohibits SecurTest from misrepresenting its participation in any	Data transfers under the EU-U.S. and Swiss-U.S. Privacy Shield framework.	FTC Takes Action against Companies Falsely Claiming Compliance with the EU-U.S. Privacy Shield, Other International Privacy Agreements	

		privacy or security program sponsored by a government, self-regulatory, or standard-setting organization, including the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield frameworks.			
32	*FTC v. AlliedWallet Inc.*, No. 2:19-cv-4355 (C.D. Cal. May 20, 2019)	Defendants alleged to have knowingly processed payments and hidden the activities of fraudulent merchants, including those of Stark Law, MOBE and Digital Altitude, which were subject to FTC enforcement actions. Pursuant to settlements, a $110 million monetary judgment was entered against Allied Wallet and its CEO, and Allied Wallet's COO was banned from payment processing and ordered to pay $1 million to the FTC.	Defendants Allied Walled Ltd. and GTBill, Ltd. are U.K. companies.	Operators of Payment Processing Firm Settle Charges for Assisting Fraudulent Schemes that Took More than $110 Million from Consumers	
33	*U.S. v. Musical.ly Inc.*, No. 2:19-cv-1439 (C.D. Cal. Feb. 27, 2019)	Defendants, operators of the social networking app Musical.ly (now known as TikTok), were alleged to have illegally collected personal information from	Defendant, Musical.ly is a Cayman Islands corporation, with its principal place of business in Shanghai, China.	Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law	

		children in violation of COPPA. Despite being aware that children were using the app, defendants also allegedly failed to obtain parental consent required under COPPA. As part of a settlement, Defendants were ordered to pay a $5.7 million penalty, comply with COPPA, and remove all videos made by children under the age of 13.			
2018					
34	*FTC v. Apex Cap. Grp., LLC*, No. CV18-09573-JFW(JPRx) (C.D. Cal. Nov. 13, 2018) (complaint amended May 30, 2019)	Defendants were alleged to have run a multi-national internet scheme that offered "free trials" for personal care products and dietary supplements, but then charged consumers full price and enrolled them in negative option continuity plans without their consent. The Defendant established shell companies in the U.S. and UK to open merchant accounts, and processed payments	Defendants used shell companies in the U.K. and a Latvia payment processor to process millions of dollars in consumer payments.	Court Temporarily Halts International Operation that Allegedly Deceived Consumers through False Claims of "Free Trial" Offers and Imposed Unauthorized Continuity Plans	

		through a Latvian financial institution. Defendant, Apex Capital, ordered to surrender assets valued between $3 million to $6 million as part of settlement agreement. Payment processor, Transact Pro, ordered to pay $3.5 million.			
35	*In re Sanctuary Belize Litigation*, No. 1:18-cv-3309 (D. Md. Oct. 31, 2018) (complaint amended Jan. 15, 2019)	Defendants, including FTC recidivist Andris Pukke, deceptively marketed lots in what supposedly would become a luxury development in Central America known by several names, including "Sanctuary Belize," taking in more than $100 million from consumers. In August 2020, the district court issued a verdict, finding in favor of the FTC. After an appeal, the district court entered an order confirming that defendants Andris Pukke, Peter Baker, and John Usher must turn over $120.2 million as well as the corporate defendants	Multi-million dollar cross-border scheme involving property purchases in Belize. Foreign defendants located in Belize and Nevis.	At FTC's Request, Court Halts Massive "Sanctuary Belize" Real Estate Investment Scam	FTC Sending Refunds to Consumers who Invested in Deceptive Sanctuary Belize Real Estate Development Scheme Operated by Repeat Offender Andris Pukke (Aug. 16, 2023)

		and their assets to compensate their victims. Defendant Chadwick settled, turning over certain assets, and agreeing to an order limiting the types of business he can engage in. Defendant Atlantic International Bank Limited (AIBL) of Belize also alleged to have assisted and facilitated the Sanctuary Belize scheme. As part of a settlement, AIBL agreed to pay $23 million, representing approximately all of its U.S.-based assets, to settle charges that it assisted the Sanctuary Belize enterprise in deceiving U.S. consumers.			
36	*FTC v. Cardiff*, No. 5:18-cv-02104-SJO-PLA (C.D. Cal. Oct. 3, 2018) (a/k/a Redwood Scientific Technologies, Inc.)	Defendants deceptively marketed dissolvable oral film strips as smoking cessation, weight loss, and sexual performance products and enrolled consumers in auto-ship continuity plans without	Defendants violated temporary restraining order by attempting to hide their control of a Canadian company in order to hide assets.	At FTC's Request, Court Stops False Advertising and Unauthorized Billing Scheme; FTC, Law Enforcement Partners Announce New Crackdown on Illegal Robocalls	

		their express informed consent. Defendants permanently banned from engaging in multi-level marketing, robocalls, negative option sales, and marketing, advertising, or selling thin film strips.			
37	*In the Matter of mResource LLC, also d/b/a Loop Works LLC*, File No. 182-3143, Docket No. C-4663 (Sept. 27, 2018)	Respondents alleged to have falsely claimed to be certified under the EU-U.S. Privacy Shield framework.	Data transfers under the EU-U.S. Privacy Shield framework.	FTC Reaches Settlements with Four Companies That Falsely Claimed Participation in the EU-U.S. Privacy Shield	
38	*In the Matter of VenPath Inc.*, File No. 182-3144, Docket No. C- 4664 (Sept. 27, 2018)	Respondents alleged to have falsely claimed to be certified under the EU-U.S. Privacy Shield framework.	Data transfers under the EU-U.S. Privacy Shield framework.	FTC Reaches Settlements with Four Companies That Falsely Claimed Participation in the EU-U.S. Privacy Shield	
39	*In the Matter of IDmission LLC*, File No. 182-3150, Docket No. C-4665 (Sept. 27, 2018)	Respondents alleged to have falsely claimed to be certified under the EU-U.S. Privacy Shield framework.	Data transfers under the EU-U.S. Privacy Shield framework.	FTC Reaches Settlements with Four Companies That Falsely Claimed Participation in the EU-U.S. Privacy Shield	
40	*In the Matter of SmartStart Emp. Screening, Inc.*, File No. 182-3154, Docket	Respondents alleged to have falsely claimed to be certified under the EU-U.S. Privacy Shield framework.	Data transfers under the EU-U.S. Privacy Shield framework.	FTC Reaches Settlements with Four Companies That Falsely Claimed Participation in the EU-U.S. Privacy Shield	

	No. C-4666 (Sept. 27, 2018)				
41	*FTC v. Apartment Hunters, Inc.*, No. 8:18-CV-1636 (C.D. Cal. Sept. 11, 2018) (also d/b/a Wetakesection8.com)	Defendants made false or unsubstantiated claims in the marketing of online rental listings offered through their websites, targeting low-income families, elderly, and disabled persons. Pursuant to a litigated final judgment and order, Defendants were ordered to pay more than $6 million and permanently banned from offering rental listing services.	Defendant UAB Apartment Hunters LT is a Lithuania company.	Court Temporarily Halts Operators of Rental Listing Websites from Making False Claims About the Availability of Apartments That Accept Section 8 Vouchers and Other Rental Properties	Court Orders Operators of Deceptive Rental Listing Websites to Pay $6 Million, Permanently Bans Them from Offering Rental Listings (Dec. 16, 2019)
42	*In the Matter of BLU Products, Inc.*, File No. 172-3025, Docket No. C-4657 (Sept. 6, 2018)	Respondents alleged to have allowed a China-based third-party service provider to collect detailed personal information about consumers, such as text message contents and real-time location information, without their knowledge or consent despite promises by the company that it would keep such information secure and private.	Data transmitted to Chinese third party without consent or notice.	Mobile Phone Maker BLU Reaches Settlement with FTC over Deceptive Privacy and Data Security Claims	

		As part of a settlement, respondents are prohibited from misrepresenting the extent to which they protect the privacy and security of personal information, and BLU will be subject to third-party assessments of its security program for 20 years.			
43	*In the Matter of ReadyTech Corp.*, File No. 182-3100, Docket No. C-4659 (July 2, 2018)	Respondent alleged to have falsely claimed that it was in the process of certifying its compliance under the EU-U.S. Privacy Shield framework. As part of a settlement, the company is prohibited from misrepresenting its participation in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including the EU-U.S. Privacy Shield framework and the Swiss-U.S. Privacy Shield framework.	Data transfers under the EU-U.S. Privacy Shield framework.	California Company Settles FTC Charges Related to Privacy Shield Participation	

44	*FTC v. Triangle Media Corp.*, No.18cv1388-MMA (NLS) (S.D. Cal. June 25, 2018) (complaint amended Dec. 11, 2018)	Defendants, who marketed and sold various products online to consumers in the United States, such as skin creams, e-cigarettes, and dietary supplements, were alleged to have deceptively advertised "risk-free" trial offers and enrolled consumers in expensive continuity plans without their knowledge or consent. Pursuant to settlements, the defendants are barred from misrepresenting any material facts about a negative option transaction, must comply with the Restore Online Shoppers' Confidence Act (ROSCA), and turn over more than $9 million in assets.	One of the principal defendants, Hardwire Inc., was a British Virgin Islands company. Defendant Global Northern Trading Limited was a Canadian company. Defendants Hardwire Interactive, Global Northern Trading, and Devin Keer helped to operate the scheme from outside the United States.	Online Marketers Barred from Deceptive "Free Trial" Offers, Unauthorized Billing	FTC Sending Refund Checks Totaling More Than $8.7 Million to Consumers Defrauded by Deceptively Marketed Online "Risk-Free Trial" Offers (June 22, 2020)
45	*FTC v. 9140-9201 Quebec Inc.*, No. 1:18-cv-04115 (N.D. Ill. June 13, 2018) (a/k/a Premium Business Pages, Inc.)	Defendants, based in Canada and the United States, made unsolicited calls to small businesses and other organizations to induce them to pay for unordered internet directory listings, search engine optimization	Canadian-based defendants targeted consumers in the United States. The FTC also received assistance from the Canada Competition Bureau.	FTC, BBB, and Law Enforcement Partners Announce Results of Operation Main Street: Stopping Small Business Scams Law Enforcement and Education Initiative	

		services, or website design and hosting services. The court ordered defendants to pay more than $4.6 million and permanently banned them from advertising, marketing, or selling any directory listings, search engine optimization services, or website design and hosting services.			
46	*FTC v. MOBE Ltd.*, No. 6:18-cv-862-Orl-37DCI (M.D. Fla. June 4, 2018)	Defendants, operators of an international organization that targeted U.S. consumers through online ads, social media, direct mailers, and live events, were alleged to have falsely claimed that their business education program called MOBE ("My Online Business Education") would help consumers start their own business and earn substantial income, taking in more than $125 million from thousands of consumers. Key perpetrators of the scheme Defendants agreed to pay more than $17	Defendants included foreign companies from Canada, the U.K., Panama, Mauritius, and Australia.	FTC Action Halts MOBE, a Massive Internet Business Coaching Scheme	Federal Trade Commission Returns More Than $23 Million To Consumers Deceived by Online Business Coaching Scheme MOBE (Apr. 5, 2022)

		million as part of settlements with the FTC.			
47	*FTC v. Next-Gen, Inc.*, No. 4:18-cv-0128 (W.D. Mo. Feb. 20, 2018)	Defendants were alleged to have operated a sweepstake that deceived millions of consumers in the United States and other countries by enticing them to pay money to collect prizes that never materialized. Pursuant to a settlement, Defendants agreed to forfeit a record $30 million in cash and assets and be permanently banned from the prize promotion business.	Defendants sent tens of millions of deceptive personalized mailers to consumers around the world, including in Canada, the United Kingdom, France, and Germany.	FTC Challenges Schemes That Target or Affect Senior Citizens	U.S. Federal Trade Commission Returning Almost $25 Million to Consumers Worldwide Who Were Defrauded by Next-Gen Sweepstakes Scheme (July 19, 2022)
48	*FTC v. Digit. Altitude LLC*, No. 18-cv-00729 (C.D. Cal. Jan. 29, 2018).	Defendants alleged to have operated a multi-million-dollar business coaching scheme that deceived consumers by claiming they could earn "six figures in 90 days." As part of settlement orders, certain former officers of the scheme are permanently banned from selling businesses	Three corporate defendants were foreign (U.K.) companies operating in the United States.	FTC Obtains Court Order Halting Business Coaching Scheme	FTC Sends Nearly $4.7 Million to Victims of Digital Altitude Business Coaching Scheme (Feb. 3, 2021)

		coaching or investment opportunity services.			
49	*FTC v. Emp Media, Inc., also d/b/a Myex.com*, No. 2:18-cv-00035 (D. Nev. Jan. 9, 2018)	Defendants, operators of a revenge porn website, alleged to have posted intimate pictures of people along with their personal information without their consent. Defendants ordered to destroy all intimate images and personal information in their possession, to shut down the website permanently, and pay more than $2 million.	Principal defendant Cottelli had substantial connection to South Africa, and routinely travelled to South Africa and the Philippines. The FTC made extensive efforts to serve him domestically and abroad, receiving assistance from authorities in the U.K. about his possible whereabouts in London, before the court allowed the FTC to serve him via email.	FTC and Nevada Seek to Halt Revenge Porn Site	
50	*U.S. v. VTech Elecs. Ltd*, No. 1:18-cv-00114 (N.D. Ill. Jan. 8, 2018)	Defendants alleged to have violated COPPA by collecting personal information from children without providing direct notice to and obtaining consent from parents and failing to take reasonable steps to secure the data it collected. As part of a settlement, VTech agreed to pay $650,000.	The FTC collaborated with the Office of the Privacy Commissioner of Canada (OPC), which released its own Report of Findings. To facilitate cooperation with OPC, the FTC relied on the U.S. SAFE WEB Act.	Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act	

2017					
51	*FTC v. Montano*, 6:17-CV-2203-JA-KRS (M.D. Fla. Dec. 28, 2017)	Defendants alleged to have operated a get-rich-quick scheme bilking consumers out of millions of dollars by falsely promising consumers they could earn hundreds to thousands of dollars a day using the defendants' Mobile Money Code products. As part of a settlement, defendants agreed to a $7 million judgment and a permanent ban on marketing or selling certain types of software.	Defendant Martin Schranz is an Austrian citizen who resides in Switzerland; defendant GSD Master AG is a Swiss company.	FTC Alleges Get-Rich-Quick Scheme Bilked Consumers out of Millions with Deceptive Claims	FTC to Mail Refund Checks to Victims of Get-Rich-Quick Scheme (March 11, 2019)
52	*FTC v. A1 Janitorial Supply Corp.*, No. 1:17-cv-07790 (N.D. Ill, Oct. 30, 2017)	Defendants alleged to have called small businesses throughout the United States and Canada, offered a free sample, and then billed them for it, even when they refused the sample. A settlement imposes a $2.7 million judgment against the defendants.	Defendants marketed and sold products in Canada.	FTC Charges Office Supply Scheme with Bilking Millions of Dollars from Small Businesses for 'Free' Samples of Cleaning Products	FTC Returns More Than $2.6 Million to Small Businesses Targeted by Office Supply Scheme (Dec. 17, 2019)

53	*In the Matter of Decusoft, LLC*, File No. 172-3173, Docket No. C-4630 (Sept. 8, 2017)	Respondent alleged to have falsely claimed participation in the EU-U.S. Privacy Shield framework.	Data transfers under the EU-U.S. Privacy Shield framework.	Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework	
54	*In the Matter of Tru Commc'n, Inc.*, File No. 172-3171, Docket No. C-4628 (Sept. 8, 2017)	Respondent alleged to have falsely claimed participation in the EU-U.S. Privacy Shield framework.	Data transfers under the EU-U.S. Privacy Shield framework.	Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework	
55	*In the Matter of Md7, LLC*, File No. 172-3172, Docket No. C-4629 (Sept. 8, 2017)	Respondent alleged to have falsely claimed participation in the EU-U.S. Privacy Shield framework.	Data transfers under the EU-U.S. Privacy Shield framework.	Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework	
56	*FTC v. Bob Robinson, LLC*, No. 17 CV 2411 (S.D. Tex. Aug. 7, 2017)	Defendants alleged to have operated a scheme to lure consumers into buying an online system, falsely promising they would earn thousands of dollars working from home. As part of a settlement, a $35.1 million judgment was imposed on the defendants.	Defendant Mega Export 2005 (Mega Canada) is a Canadian corporation.	FTC Obtains Temporary Restraining Order Halting Work-at-Home Scheme	FTC Returns More than $1 Million to Victims of Bobby J. Robinson's Work-at-Home Scheme (Apr. 16, 2019)
57	*FTC v. Vylah Tec LLC*, No. 2:17-cv-228-FtM-	Defendants alleged to have caused consumers'	N/A	FTC and Federal, State and International Partners	

	99MRM (M.D. Fla. May 1, 2017)	computers to appear as if they were infected with viruses, were being hacked, or otherwise compromised and then represented themselves as agents of Microsoft or other technology companies to persuade consumers to pay hundreds of dollars for tech support services.		Announce Major Crackdown on Tech Support Scams (May 12, 2017)	
58	*FTC v. Repair All PC, LLC.* No. 1:17-cv-0869 (N.D. Ohio Apr. 24, 2017)	Defendants alleged to have caused consumers' computers to appear as if they were infected with viruses, were being hacked, or otherwise compromised and then represented themselves as agents of Microsoft or other technology companies to persuade consumers to pay hundreds of dollars for tech support services. Settlement imposed a $12.4 million judgment and barred defendants from offering tech support products and services.	Defendant, I Fix PC, is a Canadian business. Investigation included cooperation with international law enforcement partners.	FTC and Federal, State and International Partners Announce Major Crackdown on Tech Support Scams	
59	*In the Matter of SpyChatter, Inc.*, File	Respondent alleged to have deceived consumers	Data transfers under the Asia-Pacific Economic	Three Companies Settle FTC Charges that They Deceived	

	No. 162-3251, Docket No. C-4614 (Feb. 22, 2017)	about their participation in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system.	Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system.	Consumers About Participation in International Privacy Program	
60	*In the Matter of Sentinel Labs, Inc.*, File No.162- 3250, Docket No. C-4608 (Feb. 22, 2017)	Respondent alleged to have made deceptive statements that they participated in the APEC CBPR and falsely claimed that it was a participant in a TRUSTe privacy program.	Data transfers under the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system.	Three Companies Settle FTC Charges that They Deceived Consumers About Participation in International Privacy Program	
61	*In the Matter of Vir2us, Inc.*, File No. 162-3248, Docket No. C-4609 (Feb. 22, 2017)	Respondent alleged to have made deceptive statements that they participated in the APEC CBPR.	Data transfers under the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system.	Three Companies Settle FTC Charges that They Deceived Consumers About Participation in International Privacy Program	
62	*FTC v. PHLG Enters., LLC.*, No. 8:17-cv-00220-RAL-AEP (M.D. Fla. Jan. 27, 2017)	Defendants alleged to have helped telemarketers in India deceive American consumers into paying hundreds or thousands of dollars for taxes they did not owe, or fees for services they did not receive. As part of a settlement, a $1.5 million monetary judgment was imposed on defendants.	The defendants and their runners kept a portion of the money and delivered the rest to India-based scammers through a complex series of transactions designed to avoid detection by law enforcement.	FTC Settlement Puts a Stop to Money Mule Who Profited from India-Based IRS and Other Scams	

63	*FTC v. Western Union Co.*, No. 1:17-cv-00110-CCC (M.D. Pa. Jan. 19, 2017)	Defendant alleged to have willfully failed to maintain an effective anti-money laundering program and aided and abetted wire fraud. Defendant agreed to a monetary judgment of $586 million.	Case involved assets sent abroad, with international as well as U.S. victims, and significant international cooperation, including from the Toronto Police Service, Canadian Anti-Fraud Centre, Royal Canadian Mounted Police and Spanish National Police.	Western Union Admits Anti-Money Laundering Violations and Settles Consumer Fraud Charges, Forfeits $586 Million in Settlement with FTC and Justice Department	First Round of Refunds Totaling $153 Million Sent to Consumers as a Result of Multi-Agency Case Against Western Union (March 10, 2020) Second Round of Refunds, totaling $147 Million, Sent to Consumers as a Result of Multi-Agency Case Against Western Union (Sept. 23, 2020)
64	*FTC v. D-Link Corp.*, No. 3:17-cv-00039 (N.D. Ill. Jan. 5, 2017)	Defendants alleged to have inadequately maintained proper security for its wireless routers and internet cameras. As part of a settlement, defendant D-Link was required to implement a comprehensive software security program and obtain biennial, independent, third-party assessments of its software	The FTC's initial complaint named the Taiwanese parent of D-Link.	FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras	

		security program for 10 years.			
2016					
65	*FTC v. Ruby Corp., also doing business as AshleyMadison.com*, No. 1:16-cv-02438 (D.D.C. Dec. 14. 2016)	Defendants, operators of a dating website, were alleged to have used fake profiles to entice customers to pay for memberships and failed to protect 36 million users' account and profile information in relation to a massive July 2015 data breach of their network. A $8.75 million judgment was imposed on the defendants as part of settlement.	Principal defendant was a Canadian corporation. Investigation involved cooperation with Canadian and Australian Privacy Commissioners. Defendant's website, AshleyMadison.com, had members from over 46 countries.	Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information	FTC Earns Prestigious International Award for AshleyMadison.com Data Breach Investigation (Sept. 27, 2017)
66	*FTC v. Glob. Access Tech. Support LLC*, No. 4:16-cv-01556-HEA (E.D. Mo. Oct. 3, 2016)	Defendants alleged to have operated a multi-national tech support company which used deceptive pop-up internet ads to scare thousands of consumers into paying hundreds of dollars for unnecessary technical support services. As part of a settlement, defendants agreed to turn over assets valued at more	India-based defendant and call center.	FTC Charges Tech Support Companies With Using Deceptive Pop-Up Ads to Scare Consumers Into Purchasing Unneeded Services	FTC Sending Refunds to Victims of Tech Support Scam (Aug. 1, 2019)

		than $1 million and were banned from marketing or promoting any technical support products or services.			
67	*FTC v. Somenzi*, No. 2:16-cv-07101, (C.D. Cal. Sept. 21, 2016)	Defendants used international mail network to operate a fake prize scam. As part of a settlement, a $800,000 judgment was imposed against defendant Ian Gamberg. A judgment also ordered defendants Raff and Millenium Direct were required to pay $501,895 and banned them from the prize promotion business.	Case brought as part of an international initiative targeting mass mail fraud and involved cooperation with foreign counterpart agencies.	FTC Charges Fake Prize Scheme Operators with Fraud	
68	*FTC v. OMICS Grp. Inc.*, No. 2:16-cv-02022 (D. Nev. Aug. 25, 2016)	Defendants, online publishers of hundreds of purported academic journals, deceived academics and researchers about the nature of its publications and hid publication fees ranging from hundreds to thousands of dollars. A judgment of $50.1 million judgment was	India-based defendants.	FTC Charges Academic Journal Publisher OMICS Group Deceived Researchers	

		imposed against the defendants.			
69	*FTC v. Big Dog Sol. LLC, also d/b/a Help Desk National*, No. 1:16-cv-06607 (N.D. Ill, June 24, 2016)	Defendants ran an international tech support scam duping victims into paying hundreds of dollars for dubious computer "repairs" and antivirus software. Nearly $10 million monetary judgment entered against defendants as part of settlement.	Several defendants based in Canada. This matter was also part of a coordinated effort with international partners to crackdown on tech support scams which included working with authorities in India.	FTC and Florida Charge Tech Support Operation with Tricking Consumers Into Paying Millions for Bogus Services	FTC to Provide Refunds to Victims of Tech Support Scam (Jan. 30, 2018)
70	*U.S. v. InMobi Pte Ltd.*, No. 3:16-cv-3474 (N.D. Cal. June 22, 2016)	Defendant, operator of a mobile advertising network, alleged to have deceptively tracked the locations of hundreds of millions of consumers – including children – without their knowledge or consent to serve them geo-targeted advertising. As part of settlement, defendant was subject to a $4 million civil penalty and defendant was required to delete all information it collected from children.	Singapore-based defendant.	Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission	

71	*In the Matter of Very Incognito Techs., Inc., also d/b/a Vipvape*, File No. 162-3034, Docket No. C-4580 (May 4, 2016)	Respondent alleged to have Deceived consumers about its participation in the APEC CBPR system.	Data transfers under the APEC CBPR system.	Hand-Held Vaporizer Company Settles FTC Charges It Deceived Consumers About Participation in International Privacy Program	
72	*In the Matter of ASUSTek Comput., Inc.*, File No. 142-3156, Docket No. C-4587 (Feb. 23, 2016)	Respondent alleged to have critical security flaws in its routers put home networks of hundreds of thousands of consumers at risk and routers' insecure "cloud" services led to the compromise of thousands of consumers' connected storage devices, exposing their sensitive personal information on the internet. Defendant required to establish and maintain a comprehensive security program subject to independent audits for the next 20 years as part of a settlement.	Taiwan-based defendant.	ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk	
73	*FTC v. Stratford Career Inst., Inc.*, No. 1:16-cv-00371 (N.D. Ohio Feb. 18, 2016)	Defendant alleged to have misled consumers about its online high school equivalency program that failed to meet the basic	Defendant based in Quebec, Canada.	FTC Files Action Against Stratford Career Institute for Misleading Consumers	

		requirements set by most states. Settlement imposed a $6.5 million judgment against the defendant and defendant was required to notify its current students of their right to cancel enrollment in the high school diploma program.		About Online High School 'Diploma' Course	
2015					
74	*FTC v. Click4Support, LLC*, No. 2:15-cv-05777-SD (E.D. Pa. Oct. 26, 2015)	Defendants alleged to have run a tech support scam that bilked consumers out of more than $17 million by pretending to represent Microsoft, Apple and other major tech companies. As part of settlement, defendants are banned from marketing technical support services and ordered to pay more than $554,000 and forfeit $1.3 million.	Amended complaint added an India-based defendants.	FTC, Pennsylvania and Connecticut Sue Tech Support Scammers That Took More Than $17 Million From Consumers	FTC Sends Refund Checks to Tech Support Scam Victims (Feb. 25, 2020)
75	*In the Matter of Am. Int'l Mailing, Inc.*, File No. 152-3051, Docket	Respondent alleged to have falsely claimed that they were currently certified under the U.S.-	Data transfers under the U.S.-EU Safe Harbor Privacy Framework and	FTC Settles with Two Companies Falsely Claiming to Comply with International	

	No. C-4526 (May 20, 2015)	EU Safe Harbor Privacy Framework and U.S.-Swiss Safe Harbor Privacy Framework, when in fact their certifications had lapsed years earlier.	U.S.-Swiss Safe Harbor Privacy Framework.	Safe Harbor Privacy Framework	
76	*In the Matter of TES Franchising, LLC*, File No. 152-3015, Docket No. C-4525 (May 20, 2015)	Respondent alleged to have falsely claimed that they were currently certified under the U.S.-EU Safe Harbor Privacy Framework and U.S.-Swiss Safe Harbor Privacy Framework, when in fact their certifications had lapsed years earlier.	Data transfers under the U.S.-EU Safe Harbor Privacy Framework and U.S.-Swiss Safe Harbor Framework.	FTC Settles with Two Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework	
77	*FTC v. Mail Tree Inc.*, No. 0:15-cv-61034-JIC (S.D. Fla. May 18, 2015)	Defendants alleged to have conducted a fraudulent sweepstakes scam, by mailing personalized letters soliciting payments of $20-$30 in exchange for false large cash awards of typically, more than $2 million.	Global scam with victims located in Australia, Canada, France, Germany, Japan, and the U.K. Enforcement cooperation with the Vancouver Police Department, the Windsor (Ontario) Police Service, and the Metropolitan Police in the United Kingdom.	FTC Action Halts Global Sweepstakes Scam	
78	*FTC v. Coorga Nutraceuticals Corp.*, No 15-CV-72-S (D. Wyo. May 13, 2015)	Defendants made unfounded claims that their products could prevent or reverse gray hair.	Defendant Coore claimed that two products were approved by Health Canada.	FTC Challenges Marketers' Baseless Claims That Their Supplements Prevent or Reverse Gray Hair	

		Defendants ordered to pay $391,335 as part of summary judgment against them.			
79	*FTC v. DIRECTV*, No. 3:15-cv-01129 (N.D. Cal. Mar. 11, 2015)	Defendants alleged to have made misleading representations about pricing for direct-to-home digital television services.	FTC moved for an order to serve a deposition subpoena on a witness in Spain.	FTC Charges DIRECTV with Deceptively Advertising the Cost of Its Satellite Television Service	
80	*FTC v. Am. Yellow Browser, Inc.*, No. 15-CV-2047 (N.D. Ill. Mar. 9, 2015) (a/k/a Medical Yellow Directories, Inc.)	Defendants defrauded medical practices, churches, and retirement homes by running a business directory scam where they misrepresented that consumers have agreed to buy a business directory listing and owe them money. Defendants were banned from the directory business and ordered to pay more than $1.2 million.	Three defendants were based in Montreal, Canada.	FTC Halts Online 'Yellow Pages' Scammers	
81	*FTC v. Lasarow*, No. 1:15-cv-01614 (E.D. Ill. Feb. 23, 2015) (a/k/a Mole Detective)	Defendants alleged to have made deceptive claims that their mobile apps could detect symptoms of melanoma.	Defendant L Health Ltd. is a U.K. company.	FTC Cracks Down on Marketers of "Melanoma Detection" Apps	
2014					

82	*In the Matter of True Ultimate Standards Everywhere, Inc., also d/b/a TRUSTEe, Inc.*, File No. 132-3219, Docket No. C-4512 (Nov. 17, 2014)	Respondents alleged to have deceived consumers about its recertification program, which provides seals to businesses that meet specific requirements for consumer privacy programs such as COPPA and the U.S.-EU Safe Harbor Privacy Framework. Defendants required to pay $200,000 as part of settlement.	Data transfers under the U.S.-EU Safe Harbor Framework.	TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program	
83	*FTC v. Diversified Educ. Res., LLC, also d/b/a Jefferson High School Online*, No. 0:14-cv-62116-JIC (S.D. Fla. Sept. 16, 2014)	Defendants alleged to have marketed and sold fake high school diplomas online and fabricated an accrediting body to give legitimacy to the diploma mill operation.	Foreign defendants based in Mexico and St. Kitts and Nevis.	FTC Action Halts Online High School Diploma Mill That Made $11 Million Selling Worthless Diplomas to Students	
84	*FTC v. CWB Servs.*, No. 4:14-cv-00783-DW (W.D. Mo. Sept. 5, 2014)	Defendants alleged to have bilked consumers out of tens of millions of dollars by trapping them into payday loans they never authorized and then using the supposed "loans" as a pretext to take money from their bank accounts.	Defendant Sandpoint Capital LLC was a Nevis-based company.	FTC Action Halts Payday Loan Scheme That Bilked Tens of Millions From Consumers By Trapping Them Into Supposed "Loans" They Never Authorized	FTC Returns Money to Consumers Harmed in Alleged Payday Loan Scheme (Feb. 15, 2018)

		Judgments of $32 million and $22 million imposed against defendants, Coppinger and his companies and Rowland and his companies, respectively as part of settlement.			
85	*FTC v. OnlineYellow PagesToday.com, Inc.*, No. 2:14-cv-00838-RAJ (W.D. Wash. June 9, 2014)	Defendants alleged to have defrauded millions of dollars from businesses, churches, nonprofits and local governments by charging them for unwanted listings in online "yellow pages" directories. As part of settlement, a $3,081,969 monetary judgment was imposed on the defendants.	Multiple Canadian defendants.	FTC and Florida Halt Internet 'Yellow Pages' Scammers	
86	*FTC v. 7051620 Canada, Inc.*, No. 1:14-CV-22132-FAM (S.D. Fla. June 9, 2014)	Defendants alleged to have defrauded millions of dollars from small businesses, churches, nonprofits and local government agencies by charging them for unwanted listings in online "yellow pages" directories.	Defendant 7051620 Canada, Inc. is a Canadian corporation.	FTC and Florida Halt Internet 'Yellow Pages' Scammers	

		As part of settlement, defendants were ordered to pay $1.7 million.			
87	*FTC v. First Consumers, LLC*, No. 14-1608 (E.D. Pa. Mar. 18, 2014)	Defendants alleged to have impersonated government and bank officials to defraud consumers of their bank account information. The defendants used that information to create checks drawn on consumers' bank accounts and then deposit the "remotely created checks" into corporate accounts established in the United States before transferring the money to accounts controlled by Canadian defendants. Settlement agreements with defendants Ferry and Barczi imposed judgments of $9,655,638 and $325,449 respectively. Summary judgment entered against Ari Tietolman and the corporate entities imposed a judgment of $10.7 million.	Canadian defendants.	FTC Stops Mass Telemarketing Scam That Defrauded U.S. Seniors and Others Out of Millions of Dollars	

2013					
88	*FTC v. Loewen*, No. 12-cv-1207 MJP, (W.D. Wash. Dec. 2, 2013) (a/k/a Vehicle Stars)	Defendants duped consumers into paying hundreds of dollars based on false claims that the defendants had buyers lined up for their cars. A federal court ordered the defendants to pay more than $5.1 million and banned the defendants from telemarketing and payment processing.	The defendants are Loewen, a Canadian telemarketer, and the four companies he owns. American and Canadian consumers were harmed by the telemarketing scheme. The FTC received assistance of Business Practices and Consumer Protection Authority, British Columbia, Canada.	At FTC's Request, Telemarketer Ordered to Pay $5.1 Million to Reimburse Victims of Car-Buying Scam	
89	*FTC v. Mod. Tech. Inc., also d/b/a Online Local Yellow Pages*, No. 13cv8257, (N.D. Ill. Nov. 18, 2013)	Defendants bilked millions of dollars from small businesses and churches by charging them for unwanted listings in online "yellow pages" directories. Defendants often bullied consumers into paying by threatening to sue them or damage their credit ratings. A judgment of more than $15.6 million was entered against the defendants.	The company and defendant Kaddoura operated out of Montreal, Canada, using shell companies and mail drops in the United States to hide their location. The FTC obtained cooperation from the Canadian Anti-Fraud Centre, the Kahnawake Mohawk Peacekeepers, Royal Canadian Mounted Police and the Centre of Operations Linked to Telemarketing Fraud.	FTC Stops Online 'Yellow Pages' Scam; Canada-Based Operation Targeted Small Businesses and Churches in United States	FTC Returns Money to Consumers Conned into Paying for Business Directory Listings (Dec. 4, 2015)
90	*FTC v. Applied Mktg. Scis., LLC*, No. CV13-06794 CAS (CWX),	Defendants alleged to have operated a sweepstakes scam that	Defendants sent nearly 800,000 letters to consumers in 156	FTC Sues to Stop Massive Sweepstakes Scam	

	(C.D. Cal. Sept. 16, 2013)	took more than $11 million from consumers by mass mailing personalized letters to millions of consumers and fraudulently telling them that they had won a large cash prize, typically more than $2 million, in exchange for a fee of $20 to $30. As part of a settlement, defendants were banned from any conduct involving prize promotions and a judgment of more than $11 million was imposed.	countries around the world. The FTC obtained cooperation from the Vancouver Police Department, the Metropolitan Police in the U.K, the National Fraud Intelligence Bureau, and the Australian Competition and Consumer Commission.		
91	*FTC v. AFD Advisors, LLC*, No. 13-cv-6420 (N.D. Ill. Sept. 9, 2013)	Defendants alleged to have operated a medical discount telemarketing scheme that scammed seniors by convincing them to give over their bank account information to continue receiving their Medicare, Social Security, or other insurance benefits. Defendants alleged to have used the victims' bank account information to debit	Numerous defendants were Canadian corporations or owners of those Canadian corporations. The FTC received assistance from the Canadian Anti-Fraud Centre; Royal Canadian Mounted Police; and the Centre of Operations Linked to Telemarketing Fraud.	FTC Cracks Down On Bogus Medical Discount Scam Targeting Seniors	

		money from victims' accounts. As part of settlement, a judgment over $1 million was imposed on certain defendants. A monetary judgment of nearly $900,000 was entered against other defendants.			
92	*FTC v. Money Now Funding, LLC.*, No. CV-13-01583-PHX-ROS, (D. Ariz., Aug. 5, 2013)	Defendants alleged to have falsely promised consumers that they could make money by referring merchants in their area to the defendants' non-existent money-lending service. Various judgments against and settlements with the 18 defendants imposed a ban on selling business or work-at-home opportunities and imposed a monetary judgment of $7.3 million against 12 defendants and smaller judgments against the others.	Defendants have marketed and sold home-based business opportunities to consumers throughout the United States and Canada.	FTC Halts Elusive Business Opportunity Scheme	FTC Returns Money to Victims of Business Opportunity Scheme (Feb. 17, 2017)
93	*FTC v. Vacation Commc'ns Grp., LLC.*, 6:13-cv-00789-RBD-	Defendants alleged to have operated a fraudulent timeshare resale scam where timeshare owners	Defendant Cohen conducted business from	FTC and Dozens of Law Enforcement Partners Halt Travel and Timeshare Resale	

	DAB (M.D. Fla. May 20, 2013)	were tricked into paying up-front fees based on claims that interested buyers ready to pay top dollar for the properties. Monetary judgment of over $10 million imposed on defendants Cohen and his company Vacation Communications Group LLC.	the Dominican Republic.	Scams in Multinational Effort	
94	*FTC v. Construct Data Publishers, a.s. d/b/a Fair Guide*, No. 13-CV-1999, (N.D. Ill. Mar. 14, 2013)	Defendants alleged to have tricked small businesses and non-profits into collectively paying millions of dollars to be listed in an online directory in which they had no interest in being listed and for which they did not understand they would be charged.	Defendant Construct Data Publishers a.s. is a foreign business operating out of Slovakia. Individual defendants Valdova and Anhorn were foreign defendants also based in Slovakia. The FTC obtained cooperation from the Ministry of Justice of the Republic of Slovakia, the Slovak Police Attaché, and the Ministry of Justice of Austria.	FTC Stops Foreign Operation That Scammed Many Small Businesses and Nonprofits Into Paying Millions of Dollars for Bogus Online Directory	FTC Returns Money to Victims of Business Directory Scheme (Mar. 28, 2017) *See also*, U.S. Department of Justice Press Release, Slovakian Man Indicted for Business Directory Scam (Dec. 19, 2014)
2012					
95	*FTC v. E.M.A Nationwide, Inc., d/b/a EMA and Expense Mgmt. of Am.*, No. 1:12-cv-02394-JG	Defendants alleged to have deceived consumers through a telemarketing scheme designed to sell them phony mortgage	The matter included multiple Canadian defendants. The FTC also received cooperation from Canada law enforcement agencies including the	FTC Cracks Down on Phony Mortgage Relief Schemes	FTC Mails Refund Checks Totaling Nearly $3 Million to Consumers Victimized by Alleged Mortgage

	(N.D. Ohio Sept. 25, 2012)	assistance and debt relief programs. Court order permanently bars the defendants from working in the debt relief or mortgage assistance industries and imposes a monetary judgment of $5.7 million.	Royal Canadian Mounted Police.		Relief Scam (May 28, 2014) FTC Returns $1.87 Million to Consumers Harmed by Debt Relief Scam (May 9, 2016)
96	*FTC v. Marczak, d/b/a Virtual PC Sols.*, No. 1:12-cv-07192-PAE (S.D. N.Y. Sept. 24, 2012)	Defendants alleged to have operated a tech support scheme. Defendants posed as major computer security and manufacturing companies to deceive consumers into believing that their computers were riddled with viruses, spyware, and other malware, and then charged them hundreds of dollars to remotely access and fraudulently "fix" the computers. This matter was part of an international crackdown on tech support scams targeting English speakers.	The matter included an India-based defendant. The scheme targeted English-speaking consumers in Canada, Australia, Ireland, New Zealand, and the U.K.	FTC Halts Massive Tech Support Scams	
97	*FTC v. Pecon Software Ltd.*, No. 1:12-cv-	Defendants alleged to have operated a tech support scheme by posing	The matter included India-based defendants. The scheme targeted English-	FTC Halts Massive Tech Support Scams	

	07186-PAE (S.D. N.Y. Sept. 24, 2012)	as major computer security and manufacturing companies to deceive consumers into believing that their computers were riddled with viruses, spyware and other malware. Defendants then charged consumers hundreds of dollars to remotely access and fraudulently "fix" the computers. This matter was part of an international crackdown on tech support scams targeting English speakers. Defendants ordered to pay over $500,000 as part of default judgment.	speaking consumers in Canada, Australia, Ireland, New Zealand, and the U.K. The FTC also cooperated with Canada, the U.K., and Australia.		
98	*FTC v. PCCare 24/7 Inc.*, No. 1:12-cv-07189-PAE (S.D.N.Y. Sept. 24, 2012)	Defendants alleged to have operated a tech support scheme, posing as major computer security and manufacturing companies to deceive consumers into believing that their computers were infected with viruses, spyware and other malware. Defendants then charged consumers	The matter included India-based defendants and targeted English-speaking consumers in Canada, Australia, Ireland, New Zealand, and the U.K. The FTC also cooperated with Canada, UK, and Australia.	FTC Halts Massive Tech Support Scams	

		hundreds of dollars to remotely access and fraudulently "fix" the computers. This matter was part of an international crackdown on tech support scams targeting English speakers. Monetary judgment of $2.9 million imposed on defendants as part of default judgment.			
99	*FTC v. Freedom Cos. Mktg., Inc.*, No. 12-cv-5743, (N.D. Ill. July 23, 2012)	Defendants alleged to have peddled fake mortgage assistance relief to financially distressed Spanish-speaking homeowners in the United States by falsely promising to lower homeowners' monthly mortgage payments in exchange for a hefty upfront fee. A settlement order bans the defendants from marketing any mortgage assistance relief products or services.	One defendant was incorporated and headquartered in the Dominican Republic.	FTC Action Halts Dominican Mortgage Assistance Scam That Allegedly Defrauded Spanish-Speaking U.S. Homeowners of more than $2 Million	

100	*FTC v. Am. Credit Crunchers,* No. 12-cv-1028 (E.D. Ill. Feb. 13, 2012)	Defendant alleged to have worked with bogus debt collectors in India to deceive and threaten consumers into paying debts that were not owed or that defendants were not authorized to collect, taking in over $5 million over two years. A $5.4 million judgment was imposed on defendants as part of the settlement agreement.	Defendants worked with bogus debt collectors in India.	U.S. Defendants Who Allegedly Abetted Fake Debt Collector Calls from India Agree to Settle FTC Charges	FTC Returns Money to Consumers in Phantom Debt Collection Scam (May 15, 2015)
2011					
101	*FTC v. Willms,* No. 2:11-cv-00828 (W.D. Wash. May 16, 2011)	Defendants alleged to have committed fraud by luring consumers into "free" or "risk-free" offers and then charging them for products and services they did not want or agree to purchase. A $359 million judgment was imposed on defendants as part of settlement.	The FTC worked closely with Canadian law enforcement, including the Alberta Partnership Against Cross Border Fraud, in investigating this international scheme. Most of the defendants were located in Alberta. Victims of scheme of were located in United States, Canada, the United Kingdom, Australia, and New Zealand.	FTC Charges Online Marketers with Scamming Consumers out of Hundreds of Millions of Dollars with 'Free' Trial Offers	

102	*In the Matter of Google Inc.*, File No. 102-3036, Docket No. C-4336 (Mar. 30, 2011)	Defendant alleged to have used deceptive tactics and violated its privacy promises to consumers when it launched its social network, Google Buzz. Defendant also alleged to have violated the substantive privacy requirement of the U.S.-EU Safe Harbor Framework. As part of a settlement, defendant is required to conduct independent privacy audits for the next 20 years.	Data transfers under the U.S-EU Safe Harbor Privacy framework.	FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network	
2010					
103	*U.S. v. Allied Interstate, Inc.*, No. 0:10-cv-04295-PJS-AJB (D. MN. Oct. 21, 2010)	Defendant alleged to have continued debt collection efforts after consumers told the company they did not owe the debt, without verifying the accuracy of the disputed information. Defendants also alleged to have made improper harassing phone calls to consumers and to have revealed debts to third parties.	Defendant operated out of offices in the United States, Canada, India, and the Philippines.	Debt Collector Will Pay $1.75 Million to Settle FTC Charges	

		Defendants ordered to pay $1.75 million as part of settlement.			
104	*FTC v. Iovate Health Scis. USA*, No. 10-CY-587 (W.D. N.Y. July 14, 2010)	Defendants alleged to have falsely advertised that its supplements could help consumers lose weight and treat or prevent colds and other illnesses. Defendants ordered to pay $5.5 million as part of settlement.	Defendants include a Canadian parent company and another Canadian subsidiary of that company.	Dietary Supplement Maker to Pay $5.5 Million to Settle FTC False Advertising Charges	FTC Sends Refund Checks to Consumers Who Bought Dietary Supplements (Sept. 12, 2013)
105	*FTC v. Asia Pac. Telecom, Inc.*, No. 10 C 3168 (N.D. Ill. May 24, 2010)	Defendant alleged made more than 370 million calls to consumers nationwide in one year alone in violation of the Do Not Call Registry Rule.	Defendant operated out of various locations, including in the Northern Mariana Islands, Hong Kong, and the Netherlands.	At FTC's Request, Court Halts Massive Robocall Operation (June 10, 2010)	
106	*FTC v. Advanced Mngt. Servs. NW LLC*, No. CV-10-0148-LRS (E.D. Wa. May 10, 2010)	Defendants alleged to have made calls to consumers nationwide, claiming that they could negotiate with credit card issuers to substantially lower the interest rates on the consumers' credit cards. Defendants also alleged to have delivered prerecorded "robocalls"	FTC was assisted in the investigation by Toronto Strategic Partnership, which includes as member agencies the Competition Bureau Canada, the Toronto Police Service Fraud Squad – Mass Marketing Section, the Ontario Provincial Police Anti-Rackets Section, the Ontario Ministry of Consumer Services, the	At FTC's Request, Court Stops Deceptive Telemarketing Calls Pitching Credit Card Interest Rate Reduction (May 20, 2010)	

		that consisted of urgent-sounding messages.	Royal Canadian Mounted Police, and the U.K.'s Office of Fair Trading.		
2009					
107	*FTC v. MoneyGram Int'l,* No. 1:09-cv-06576 (N.D. Ill. Oct. 19, 2009)	Defendants alleged to have allowed their money transfer system to be used by fraudulent telemarketers to bilk consumers out of tens of millions of dollars. Defendants settled the charges. In 2018, the company agreed to pay $125 million to settle allegations that it failed to take steps required under the 2009 order to crack down on fraudulent money transfers that cost U.S. consumers millions of dollars.	Canadian agents allegedly used MoneyGram outlets in Canada to defraud U.S. consumers.	MoneyGram to Pay $18 Million to Settle FTC Charges That it Allowed its Money Transfer System to Be Used for Fraud	FTC Mails Redress Checks to Fraud Victims Who Lost Money Through MoneyGram's Money Transfer System (Apr. 28, 2010) Claims Process Opens for Consumers Who Were Victimized by Fraudulent MoneyGram Transfers (June 1, 2021)
108	*FTC v. Javian Karnani*, No. 09-CV-5276 (C.D. Cal. July 20, 2009) (a/k/a Best Priced Brands, LLC)	The FTC alleged that defendants deceptively advertised and sold consumer electronic products, such as cameras, video game systems, and computer software, via	The case exclusively targeted consumers in the U.K. U.K. authorities also assisted the FTC with this investigation. Many consumers in the U.K. registered complaints with	Court Halts U.S. Internet Seller Deceptively Posing as U.K. Home Electronics Site	

		the internet to consumers in the U.K.	the FTC through econsumer.gov.		
109	*FTC v. Diamond Phone Card, Inc.*, No. 09-CV-3257 (E.D.N.Y. July 29, 2009)	Defendants alleged to have 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.		
110	*FTC v. Paul Navestad*, No. 09 CV 6329T (W.D.N.Y. June 25, 2009) (a/k/a Cash Grant Institute)	Defendants alleged to have waged an automated robocall campaign promoting bogus claims that consumers were qualified for grant money from the government, private foundations, and wealthy individuals. In 2012, federal judge ordered the defendants to pay a total of $30 million in civil penalties and give up more than $1.1 million in ill-gotten gains. The court order includes a $20	The defendants conducted business through companies that were purportedly based abroad.	FTC Cracks Down on Scammers Trying to Take Advantage of the Economic Downturn	FTC Action Leads to Arrest Warrant for 'Cash Grant Institute' Robocaller Who Ignored Court Order to Pay More Than $20 Million in Penalties (Feb. 20, 2014)

		million judgment against Paul Navestad. In 2014, a federal judge ordered the arrest and incarceration of Paul Navestad for the court order.			
111	*FTC v. MCS PROGRAMS, LLC*, No. C09-5380RBL (W.D. Wa. June 25, 2009)	Defendants alleged to have used cold calls, pre-recorded "robocalls," and the internet to push a phony "Rapid Debt Reduction" program to consumers in the United States and Canada.	The scheme impacted consumers in the U.S. and Canada. The FTC also received assistance from the Canadian Competition Bureau.	FTC Cracks Down on Scammers Trying to Take Advantage of the Economic Downturn (July 1, 2009)	
112	*FTC v. In Deep Servs., Inc.*, No. 09-CV-01193 (C.D. Cal. June 23, 2009)	Defendants alleged to have 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.	FTC Cracks Down on Scammers Trying to Take Advantage of the Economic Downturn (July 1, 2009)	
113	*FTC v. Wagner Ramos Borges*, No. 09-CV-	Defendant alleged to have operated a bogus employment scam.	The defendant was allegedly located abroad.	FTC Cracks Down on Scammers Trying to Take	

	1634 (D. Md. June 22, 2009)			Advantage of the Economic Downturn (July 1, 2009)	
114	*FTC v. 6654916 Canada Inc., a Canadian Corporation, d/b/a National Yellow Pages Online Inc.*, No. 09C 3159 (N.D. Ill. 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, assisted with this investigation. The defendants were based in Canada.	FTC Sues to Halt Three Cross-Border Business Directory Scams (June 2, 2009)	
115	*FTC v. Integration Media Inc., a corporation, d/b/a GoAm Media*, No. 09C 3160 (N.D. Ill. 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, assisted with this investigation. The defendants were based in Canada.	FTC Sues to Halt Three Cross-Border Business Directory Scams (June 2, 2009)	FTC Returns Refunds to Small Businesses and Non-Profits Defrauded in Cross-Border Business Directory Scams (Nov. 3, 2021)
116	*FTC v. 6253547 Canada, Inc.*, No. 1:09CV01211 (N.D. Ill. May 27, 2009) (consolidated with FTC v. Integration Media, Inc. 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, assisted with this investigation. The		

			defendants were based in Canada.		
117	*FTC v. 6555381 Canada, Inc., a corporation, d/b/a Reed Publishing*, No. 09C 3158, (N.D. Ill. 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, assisted with this investigation. The defendants were based in Canada.	FTC Sues to Halt Three Cross-Border Business Directory Scams	
118	*FTC v. Sean Cantkier*, 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.	FTC Obtains Court Order Halting Deceptive Mortgage Relief Internet Ads; Marketers Falsely Claimed to Operate MakingHomeAffordable.gov	FTC Settlement Orders Ban More Than a Dozen Marketers from Selling Mortgage Relief Services; Repeat Offender Ordered to Pay $11.4 Million for Contempt (June 17, 2010)
119	*FTC v. Romeo*, No. 2:09-cv-01262-WJM-CCC (D.N.J. 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.	FTC Charges Marketers of Hoodia Weight Loss Supplements with Deceptive Advertising	
2008					

120	*FTC v. Innovative Mktg., Inc.*, Civil Action No. RDB 08CV3233 (D. Md. 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.	Court Halts Bogus Computer Scans	FTC To Provide Refunds to Victims of Bogus Scareware Scam (Dec. 9, 2011) Appeals Court Affirms Ruling in Favor of FTC, Upholds $163 Million Judgment Against 'Scareware' Marketer (Feb. 28, 2014)
121	*FTC v. Cash Today, Ltd.*, No. 3:08-cv00590-BES-VPC (D. Nev. Nov. 6, 2008)	Defendants alleged to have 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.	FTC Charges Internet Payday Lenders with Failing to Disclose Key Loan Terms and Using Abusive and Deceptive Collection Tactics	
122	*FTC v. CyberSpy Software, LLC*, No. 08-cv08172 (M.D. Fla. Nov. 5, 2008)	Defendants alleged to have 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.	Court Orders Halt to Sale of Spyware	
123	*FTC v. 9163-7710 Québec, Inc.*, No. 3:08-	Defendants allegedly violated the FTC Act by misrepresenting that they	This case was brought with the assistance of the Royal Canadian Mounted	FTC Stops Fake 'Yellow Pages' Marketers Who Bilked	

	CV02131-GAG (D.P.R. Oct. 28, 2008)	had preexisting relationships with consumers, that consumers had agreed to purchase defendants' services, and that consumers owed money for defendants' services	Police and Project COLT, a multi-agency, U.S.-Canada initiative formed in the 1990s to combat telemarketing fraud.	Spanish-Speaking Businesses in Cross-Border Scam	
124	*FTC v. RCA Credit Servs., LLC*, No. 8:08-CV2062-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	'Operation Clean Sweep': FTC and State Agencies Target 36 'Credit Repair' Operations	Court Finds Defendant in Contempt for Violating Prior Court Order That Prohibited Him from Making Credit Repair Pitches to Consumers (Oct. 20, 2011)
125	*FTC v. Atkinson, No. 08-CV-5666* (N.D. Ill. 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.	FTC Shuts Down, Freezes Assets of Vast International Spam E-Mail Network	Court Orders Australia-based Leader of International Spam Network to Pay $15.15 Million (Nov. 30, 2009)
126	*FTC v. Nu-Gen Nutrition, Inc.*, No. 1:08-cv- 05309 (N.D. Ill Sept. 18, 2008)	Defendants alleged to have deceptively advertised bogus cancer remedies.	Defendants sold cancer remedies to victims in foreign countries.	FTC Sweep Stops Peddlers of Bogus Cancer Cures	

127	*FTC v. Advanced Patch Techs., Inc.*, No. 1:04-CV-0670 (N.D. Ga. Mar. 10, 2004) (modified settlement Sept. 16, 2008)	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.	Marketers of Weight-Loss Patch to Pay More Than $110,000 for Violating Previous FTC Settlements	
128	*FTC v. 9107-4021 Québec, Inc., a corporation, also d/b/a Med Provisions*, No. 1:08-cv-01051- DCN (N.D. Ohio 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.	FTC Announces Operation Tele-PHONEY, Agency's Largest Telemarketing Sweep	
129	*FTC v. 6554962 Canada Inc., d/b/a Union Consumer Benefits*, No. 1:08-cv-02309 (N.D. Ill. 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.	FTC Announces Operation Tele-PHONEY, Agency's Largest Telemarketing Sweep	
130	*FTC v. NHS Sys., Inc.*, No. 08-cv-2215 (E.D. Pa. May 13, 2008)	Defendants allegedly engaged in deceptive telemarketing and unauthorized billing practices. They purported to contact consumers on behalf of government	Key defendants were based in Canada and St. Lucia. Canadian authorities assisted with serving process on some	FTC Announces Operation Tele-PHONEY, Agency's Largest Telemarketing Sweep	

		agencies and charged consumers to enroll in programs without their consent.	of the defendants located in Canada.		
131	*FTC v. Datacom Mktg.,Inc.*, No. 06 C 2574 (N.D. Ill. 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.	Court Halts Canadian Operation Charging for Unordered and Unwanted Business Directory Listings	
132	*FTC v. Data Bus. Solutions Inc.*, No. 08-CV- 2783 (ND. Ill. May 14, 2008)	Defendants alleged to have run 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	FTC Halts Cross Border Con Artists	

133	*FTC v. Alternatel, Inc.*, No. 1:08-cv-21433-AJ (S.D. Fla. 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 aided in this investigation.	FTC Halts Bogus Prepaid Phone Card Claims, Cards Failed to Deliver the Number of Minutes Promised in Ads	
134	*FTC v. Clifton Telecard Alliance One LLC*, No. 2:08-cv-1480-pgs-es (D.N.J. 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.	FTC Asks Court to Halt Prepaid Calling Card Scam; Alleges Consumers Receive Fewer Calling Minutes Than Advertised and Pay Hidden Fees	
2007					
135	*FTC v. Your Money Access, LLC*, No. 07-547 (E.D. Pa. 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	Defendants' clients included foreign entities such as Canadian telemarketers.		FTC Gets $3.6 Million Judgment Against Companies that Allegedly Debited Money from Consumers' Bank Accounts

		numerous fraudulent telemarketers and Internet-based merchants.			Without Permission (Nov. 5, 2010)
136	*FTC v. B.C. Ltd. 0763496, d/b/a Cash Corner Services, Inc.*, No. C07-1755 (W.D. Wa. 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.	Court Halts Bogus Check Scam Targeting Lottery Winners; Money Transfers Used to Defraud Consumers	FTC Sends Refunds to Consumers Defrauded by Counterfeit Check and Prize Scam (Nov. 22, 2011)
137	*FTC v. Spear Sys., Inc.*, No. 07C-5597 (N.D. Ill. Oct. 3, 2007) (complaint amended May 15, 2008)	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 antiaging products and making claims about those products that were false and unsubstantiated.	Defendants were based in Australia and Canada.	FTC Stops International Spamming Enterprise that Sold Bogus Hoodia and Human Growth Hormone Pills	Defendants in International Spam Operation Settle FTC Charges; New Canadian Defendants Identified (July 15, 2008)
138	*FTC v. Practical Mktg., Inc.*, No. 3:07-cv00685-JPG-DGW (S.D. Ill. 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	Defendants sold lists to Canadian telemarketers.	Federal Enforcers Target List Brokers	

		limits. The lists included consumers' credit card and bank account information, exposing thousands of consumers to possible identity theft, and violating federal law.			
139	*FTC v. Sili Neutraceuticals, LLC*, No. 07C 4541 (N.D. Ill. 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.	FTC Stops Spammers Selling Bogus Hoodia Weight-Loss Products and Human Growth Hormone Anti-Aging Products	
140	*FTC v. 9131-4740 Québec, Inc., a corporation, also d/b/a Fusion Telekom*, No. 07-cv-02242 (N.D. Ohio 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.	Cross-Border Telemarketers Face FTC Charges for Deceptive Phone Card Pitches	
141	*FTC v. Crystal Ewing*, FTC No. 062- 3025 (D. Nev. Apr. 11, 2007).	Defendants allegedly ran a deceptive prize promotion scheme.	Defendants targeted consumers in the United States, Canada, and the United Kingdom.	Sweepstakes Promoters Will Pay $1.4 Million To Settle FTC Charges	FTC Obtains $9.5 Million Judgment Against Sweepstakes Promoter for Contempt (Feb. 11, 2015)

142	*FTC v. Mystery Shop Link, LLC*, No. CV07-01791 SJO (Shx) (C.D. Cal. 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.	Enigma for Consumers: What Mystery Shopping Jobs?	
143	*FTC v. Select Personnel Mgmt., Inc.*, No. 07C 0529 (N.D. Ill. 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.	FTC Stops Credit Card Rate Reduction Scam	
144	*FTC v. Lane Labs-USA, Inc.*, No. 00CV3174 (D.N.J. June 29, 2000) (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.	FTC Files Civil Contempt Action Against Lane Labs Defendants	FTC Sending Refund Checks Totaling Nearly $955,000 to Consumers Who Lost Money Buying Lane Labs' AdvaCAL Calcium Supplement (Mar. 18, 2015) Lane Labs Found in Contempt of Court Order Barring Deceptive Health Claims (Nov. 18, 2011)
145	*FTC v. International Prod. Design, Inc.*, No. 1:97-CV-01114-AVB	Defendants allegedly violated a 1998 order prohibiting them from deceptively marketing	One of the original corporate defendants was	FTC Charges Invention Promotion Swindlers with Contempt	FTC Appoints Monitor to Ensure that Dow Chemical Meets all

	(E.D. Va. contempt action Jan. 8, 2007)	invention promotion services.	based in the United Kingdom.		Conditions of its 2009 Acquisition of Rohm & Haas; FTC Mails Redress Checks to Invention Promotion Scam Victims (July 9, 2010)