Innovation, Science and Economic Development Canada
Innovation, Sciences et Développement économique Canada

Canada

CANADA'S ANTI-SPAM LEGISLATION (CASL)

+ PERFORMANCE MEASUREMENT REPORT 2019-2020

This publication is available online at:
https://www.ic.gc.ca/eic/site/030.nsf/eng/00027.html

To obtain a copy of this publication, or to receive it in an alternate format (Braille, large print, etc.), please fill out the Publication Request Form at www.ic.gc.ca/Publication-Request or contact:

Web Services Centre
Innovation, Science and Economic Development Canada
C.D. Howe Building
235 Queen Street
Ottawa, ON K1A 0H5
Canada

Telephone (toll-free in Canada): 1-800-328-6189
Telephone (international): 613-954-5031
TTY (for hearing impaired): 1-866-694-8389
Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)
Email: ISED@canada.ca

Cat. No. Iu170-2E-PDF
ISSN 2562-3265

Aussi offert en français sous le titre *Initiative relative à la Loi canadienne anti-pourriel (LCAP), rapport de mesure du rendement.*

Table of Contents

1. Introduction

Canada's Anti-Spam Legislation (CASL) aims to protect Canadians from the misuse of digital technology, including spam and emerging electronic threats, all of which can impose costs, create inefficiencies, cause harm and undermine the confidence that businesses and individuals should have in the electronic marketplace.

CASL plays an important role in balancing the potential of a data-driven economy against Canadians' right to have their data and privacy protected. The legislation also aims to protect Canadians from practices that could put them at risk of fraud, identity theft and financial loss. The legislation was passed in 2010, but most provisions came into force in 2014 with a three-year transition period to give consumers and businesses time to learn about and comply with the legislation.

In the context of commercial activity, CASL's rules prohibit, among other practices:

- **spamming**—sending commercial electronic messages without prior consent;
- **deceptive marketing**—making false or misleading claims online, including in website addresses;
- **malware**—installing software without prior consent;
- **hacking**—altering transmission data;
- **address harvesting**—using computer programs to collect or use electronic addresses without prior consent; and
- **spyware and related activities**— the collection or use of individuals' personal information through unlawful access to their computer systems via any means of telecommunication.

As in past years, the 2019–2020 CASL performance measurement report aims to increase general awareness of the CASL initiative. It provides an overview of relevant performance data and government partners' roles and activities in 2019–2020.

2. CASL Partners

The CASL initiative engages multiple federal partners that have complementary mandates. Innovation, Science and Economic Development Canada (ISED) oversees the initiative, while the Canadian Radio-television and Telecommunications Commission (CRTC), Office of the Privacy Commissioner of Canada (OPC) and Competition Bureau enforce CASL or CASL-related provisions. The CASL partners' roles and responsibilities have been set out in foundational documents and legislative mandates as shown in the following diagram:

CASL Initiative

Non-Enforcement (ISED)

National Coordinating Body (NCB)

The NCB resides within ISED's Privacy and Data Protection Directorate. It:

- conducts policy oversight, including monitoring and reporting on the regime's overall effectiveness
- oversees public communication and outreach activities

Office of Consumer Affairs (OCA)

The OCA is responsible for consumer protection and promotion. It:

- coordinates consumer and business education and awareness efforts
- manages the Fightspam.gc.ca website

Enforcement

Canadian Radio-television and Telecommunications Commission (CRTC)

The CRTC is an administrative tribunal that operates at arm's length from the federal government. It:

- enforces and investigates potential violations of CASL's prohibitions against sending spam, altering transmission data and installing software on computer systems and/or networks without consent
- encourages compliance through outreach, sanctions and remedies for violations, such as administrative monetary penalties (AMPs)
- houses the Spam Reporting Centre, the central point for individuals to report spam, file complaints and alert enforcement agencies about alleged CASL violations

Competition Bureau (the "Bureau")

The Bureau is an independent law enforcement agency. Through amendments to the Competition Act, it:

- enforces and investigates cases of false or misleading electronic representations and deceptive marketing practices in the electronic marketplace, including false or misleading sender or subject matter information, electronic messages, and locator information, such as URLs and metadata
- encourages compliance through outreach, advocacy and enforcement. Under the Competition Act, CASL-related matters can be resolved through Consent Agreements, court orders, fines and monetary penalties.

Office of the Privacy Commissioner of Canada (OPC)

The OPC is an agent of Parliament. Through amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA), it:

- enforces and investigates the unauthorized collection and use of electronic addresses through the use of computer programs and of individuals' personal information through unlawful access to their computer systems or via any other means of telecommunication
- encourages compliance with CASL-related PIPEDA provisions through outreach and remedies (excluding AMPs)

3. Results at a Glance

Promoting

The Fightspam.gc.ca website, managed by the Office of Consumer Affairs (OCA), is a key tool for promoting CASL. It contains important information and resources for understanding the Act and increasing compliance. In 2019–2020, it received 234,519 visits.

CASL partners share information aimed at promoting education and compliance with the legislation—such as FAQs and other guidance material for Canadians and businesses—on their respective websites and through education and outreach activities. The partners also reach out to a variety of audiences through formal publications, blog posts and social media.

In 2019–2020:

- The CRTC's CASL-related web pages were viewed more than 224,441 times (up 75% from last year). The CRTC released 71 tweets and 14 Facebook posts, and held 37 outreach activities.
- The OPC's CASL-related web pages were viewed more than 37,316 times. The OPC also produced an insert about CASL in collaboration with Canada Revenue Agency. The insert's potential reach was 477,350 Canadian businesses.
- The Competition Bureau's CASL-related web pages were viewed more than 16,765 times. The Bureau issued 1 publication, 1 statement and 4 CASL-related consumer and business alerts, and participated in Fraud Prevention Month in March 2020.
- The OCA promoted CASL through its social media activities, including 7 posts on ISED social media channels. It also reposted 9 CRTC social media posts.

Monitoring

The CRTC hosts the Spam Reporting Centre, which collects information that can serve as evidence of potential CASL violations. In 2019–2020, Canadians made 309,985 submissions to the centre (up 10% from the previous year), including 14,809 web form submissions and 295,176 email forwards.

The Competition Bureau launched a Compliance Monitoring Unit to ensure that matters that have been resolved through consent agreements, criminal sentencing orders, alternative case resolutions or other court orders are monitored more consistently. CASL-related matters resolved by the Bureau will also be included in the compliance monitoring work conducted by the Unit.

Enforcing

The enforcement agencies have effective tools to respond to non-compliance, such as warning letters, notices of violations, undertakings and consent agreements. The CRTC can also impose and the Competition Bureau can seek administrative monetary penalties (AMPs), while the OPC can enter into compliance agreements with respondents. These tools are meant to promote and enforce compliance with CASL and CASL-related regulations.

In 2019–2020, the CRTC:

- led a complex investigation in cooperation with domestic and international law enforcement agencies and private cybersecurity firms that resulted in a successful enforcement action;
- held an individual, in their capacity as a director, liable under CASL for the first time; and
- issued a total of $115,000 in AMPs.

The OPC investigated:

- data and list brokers' privacy management practices;
- an allegation that mobile device management software had been covertly installed on an individual's cellphone;
- an allegation that remote access tool (RAT) software had been covertly installed on an individual's laptop; and
- an allegation of unsolicited email marketing.

The Competition Bureau:

- resolved 2 matters with registered consent agreements and AMPs, totalling $5.3M; and
- took action in 2 matters to stop false or misleading claims while it investigated.

4. The Environment

4.1 International Context

Companies, governments and citizens around the world are struggling to keep up with the accelerating scale and pace of technological change. The Internet's growth has provided unprecedented opportunities for people to express themselves, build networks and participate in the global economy, but it has also opened up new avenues for nefarious activities, such as hacking, denial-of-service attacks, online fraud and identity theft.

As more people and things connect to the Internet, attack surfaces (vulnerable entry points) and interdependencies grow, making it easier for fraudsters to install malware on smartphones and Internet of Things (IoT) devices. Cyber attacks have proliferated as the world becomes more and more connected.

In a globalized world, cyber threats do not respect national boundaries. Most attacks targeting Canadians originate outside the country; despite being a smaller market, Canada is a prime target for malicious online activity. These ongoing threats highlight the need for countries to cooperate to mitigate cybersecurity issues.

To that end, CASL—which is part of a broad range of domestic and international legal and policy frameworks in the areas of spectrum, telecommunications, privacy protection and cyber resilience, including cybersecurity—provides its enforcement partners with the ability to share information and cooperate including with data protection authority counterparts to protect Canadians' information domestically and abroad.

4.2 Trends and Indicators

The CASL National Coordinating Body keeps abreast of the most recent developments in spam, online threats, cybersecurity and e-commerce spheres by performing strategic intelligence scans, conducting research, and analyzing metrics and trends.

In 2019, almost a decade after CASL was enacted with the objective to ensure "the viability of e-commerce

throughout Canada" by combating spam and other electronic threats, consumers and businesses continue to be targeted by online criminal groups through online threats such as spoofing, phishing, tech support scams, ransomware attacks and others.

In 2019, 71% of organizations in Canada reported being the target of at least one cyber attack in 2019 that had caused losses, whether in terms of time and resources, out-of-pocket expenses or ransom payments. Globally, in the same year, 94% of malware was delivered by email; about 60% of the most malicious domains were associated with spam campaigns, with the majority of victims having lost money to scams being approached online or via electronic media.

Global research on online advertisement has shown that the pervasive use of ad tech and questionable targeting methods increase the public's concerns about online privacy, transparency and data control. CASL plays an important role in building trust in the digital environment by protecting Canadians while allowing organizations to have reasonable ways to communicate electronically with citizens.

In 2019, more than three quarters of Canadian business representatives (77%) said their company had taken steps to comply with Canada's privacy laws, which may explain that no operation originating in Canada figured in the Spamhaus Project's Register of Known Spam Operations database or 10 Worst Spammers list. In addition, Canada was not in the Spamhaus 10 Worst Spam Countries list or 10 Worst Botnet Countries list.

5. Results

5.1 Policy and Coordination

National Coordinating Body

In addition to the research described above, the National Coordinating Body (NCB) works with national and international partners to align legislative and regulatory frameworks with international anti-spam and malware industry best practices.

In 2019–2020, the NCB:

- participated in the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)—a spam-related international forum—alongside Canadian partners;
- informed and advised ISED (the ministry responsible for CASL) on all developments relating to CASL management and policy;
- coordinated CASL governance activities, such as Directors General Steering Committee and Working Groups, and engaged CASL partners to discuss policy and strategy;
- collaborated with CASL partners to update the Fightspam.gc.ca website;
- collaborated with Statistics Canada to update the Canadian Internet Use Survey, which provides data related to CASL performance indicators; and
- collaborated with its CASL partners to implement all actions elaborated in the Management Response and Action Plan and complete the 4 recommendations made by the Horizontal Evaluation Report.

5.2 Promoting Compliance

Canadian Radio-television and Telecommunications Commission

Complementing Fightspam.gc.ca, the CRTC's website provides additional CASL-related information to Canadians and stakeholders to make it easier for everyone to find the help they need. The online experience includes easy-to-access alerts, videos, infographics, policies and guidelines intended to inform Canadian consumers about CASL and help businesses comply. The CRTC also educates and informs stakeholders and Canadians through social media platforms, such as Twitter and Facebook.

In 2019–2020, the CRTC:

- released 71 tweets, resulting in 220,126 impressions and 194 retweets;
- made 14 Facebook posts, reaching 9,881 people and provoking 139 reactions;
- conducted more than 37 outreach activities for domestic and international stakeholders in the form of general outreach, information sessions, compliance meetings, webinars and keynote speeches, including:
  - a CASL presentation to international stakeholders at Europol
  - an address by the CRTC's Chief Compliance and Enforcement Officer to a panel on "Cybersecurity Risks and Realities" at the Telecommunications Media Forum
- published 2 CASL Enforcement Dashboards on the CRTC website;
- issued an enforcement advisory for businesses collecting customer data with in-store Wi-Fi;
- published 2 investigation summaries, one related to Orcus Technologies and one concerning Couch Commerce Inc. and nCrowd, Inc.
- issued information letters to major service providers to alert them to a vulnerability identified by the National Institute for Standards and Technology, which helped them address the potential threat and minimize the possibility of CASL violations; and
- used social media to advise Canadians to be aware of and report emerging scams related to COVID-19.

Office of the Privacy Commissioner of Canada

The OPC delivered ongoing CASL-related compliance guidance for businesses and advice for individuals through different channels. The Canada's anti-spam legislation page on the OPC's website is the Office's primary tool for sharing information with individuals and businesses, and is its most effective way to promote CASL-related activities.

The OPC also carried out CASL outreach activities throughout the year, such as sharing content through social media channels; participating, speaking and exhibiting at events across Canada; publishing and distributing material; producing videos; publishing articles in community newspapers; and running radio spots across the country.

Here are some highlights from 2019–2020:

- CASL-related web pages were viewed more than 37,316 times.
- The OPC partnered with Canada Revenue Agency to mail a printed insert about CASL to 477,350 small- and medium-sized enterprises across Canada registered under the Employer Accounts Program. The goal was to inform businesses about e-marketing spam and threats, such as those related to email, instant messaging and social media, including harvesting electronic messages. The campaign also aimed to bring businesses closer to compliance with the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and CASL.
- The OPC updated its online resources related to CASL, including those related to compliance help for businesses. In January 2020, the Office also updated its Guidance for businesses doing e-marketing. The guidance informs organizations about the OPC mandate related to electronic address harvesting and e-marketing, and helps them comply with PIPEDA when conducting e-marketing activities.
- The OPC produced an educational 2-minute video on CASL guidance aimed at businesses to inform them of their privacy obligations under PIPEDA and CASL and bring them closer to compliance with the laws. The video will be launched in 2020–2021.
- The OPC designed and printed a new Privacy Guide for Businesses that includes a section on CASL. An accessible PDF version will be posted online in 2020–2021.

- The OPC's Information Centre responded to a total of 108 CASL-related requests from individuals and businesses. The most common inquiry category was consent.

Competition Bureau

The Competition Bureau increases awareness of CASL-related issues in a number of important ways to reach as many Canadian consumers and businesses as possible.

On March 4, 2020, the Bureau published its fifth edition of the Deceptive Marketing Practices Digest. The digest focuses on 3 marketing issues that affect consumers and businesses in the online marketplace:

- the collection of consumer data in exchange for "free" online products and services;
- unsubstantiated weight loss claims; and
- the advertising of unattainable prices in the car rental market.

On March 20, 2020, the Bureau issued a statement asking Canadians to remain vigilant against potentially harmful anti-competitive conduct, including potentially false or misleading claims by businesses that their products and services can prevent, treat or cure COVID-19.

The Bureau issued 4 CASL-related consumer and business alerts in 2019–2020 to address a wide range of issues, including promo deals for telecom service agreements, subscription traps, online third-party sellers and spoofed federal government websites.

The Bureau also played an important role in Fraud Prevention Month by giving Canadians the tools they need to recognize, reject and report fraud.

Office of Consumer Affairs

The OCA manages CASL-related communication products for Canadian individuals and businesses, including the official CASL website, Fightspam.gc.ca, which promotes CASL-related information. In 2019–2020, the website received 234,519 visits (page views).

Early in this time frame, the OCA led the CASL website revitalization project, which included close collaboration with the NCB and the 3 enforcement partners. The new website, featuring updated content that is simpler in structure and language, was launched on April 1, 2019.

In addition to creating awareness online, the OCA promoted CASL through social media activities in 2019–2020. It published 7 original CASL-related posts on ISED social media channels and reposted 9 CRTC CASL-related social media posts. The original CASL social media posts attracted 33,096 impressions, while the CRTC reposts garnered 39,279.

5.3 International and Domestic Cooperation

Throughout 2019–2020, CASL enforcement partners worked with their domestic and international counterparts to promote compliance. Given the borderless nature of the Internet, CASL violations can originate outside Canadian borders. As such, international cooperation is often needed when investigating online threats. To that end, information-sharing and cooperation with foreign governments and organizations is essential to ensure effective and coherent global cooperative actions against CASL violators.

Canadian Radio-television and Telecommunications Commission

Like its CASL enforcement partners, the CRTC has forged partnerships with organizations across the globe to better fulfill its mandate.

The CRTC continues to be part of the Unsolicited Communications Enforcement Network (UCENet). Members from more than 26 countries work together to promote international spam enforcement cooperation and address problems relating to spam and unsolicited telecommunications.

As part of a complex investigation in 2019–2020, CRTC staff cooperated with domestic and international law enforcement agencies, including the RCMP, the US Federal Bureau of Investigation, the Australian Federal Police and private cybersecurity firms.

This collaboration resulted in the Chief Compliance and Enforcement Officer issuing Notices of Violation for contraventions of section 9 of CASL to Orcus Technologies and its partners, John Paul Revesz and Vincent Leo Griebel, who developed, marketed and sold the Orcus Remote Access Trojan (RAT) malware. Malicious actors could use this malware to control computer systems without the owner's consent, contrary to CASL. These enforcement actions resulted in an $115,000 penalty.

Malicious software like this can victimize citizens in multiple jurisdictions. Successful cooperation between the CRTC and law enforcement in other countries demonstrates the benefits of working together to address global threats.

Office of the Privacy Commissioner of Canada

In April 2011, CASL amended PIPEDA's provisions, enabling the OPC to collaborate and share information with its provincial and international data protection counterparts. Since then, the OPC has engaged in many joint and collaborative enforcement actions with partners through memoranda of understanding and participation in various regulatory networks. In fact, such cooperation has now become the normal course of business.

- The OPC is a member of the Executive Committee of the Global Privacy Enforcement Network (GPEN). As such, it participates in collaborative enforcement activities, hosts and administers the GPEN website and takes part in privacy-themed monthly calls and network meetings.
- In May 2019, the OPC participated and presented at the 3rd GPEN Enforcement Practitioner's Conference in Macao, which focused on international enforcement collaboration across regulatory sectors as well as best practices in the sharing of investigative techniques.
- The OPC also participated with 15 other data protection authorities in the 2019 GPEN Sweep, which examined how organizations handle and respond to data breaches.
- Finally, through GPEN, the OPC intensified its collaboration with the International Consumer Protection Enforcement Network (ICPEN). GPEN endorsed an ICPEN letter to app marketplaces calling for improved privacy transparency—representing the first global cross-regulatory collaborative effort of its kind—and participated in a meeting of ICPEN members in Cartagena, Colombia in May 2019.
- The Global Privacy Assembly (GPA), formerly known as the International Conference of Data Protection and Privacy Commissioners, is a forum for privacy and data protection authorities from around the world.
  - In addition to attending the 41st Conference in Tirana, Albania, the OPC is co-chair of the GPA's International Enforcement Collaboration Working Group, whose members are working to advance enforcement cooperation across international jurisdictions and establishing practical measures to support this.
  - The OPC also co-chairs the GPA's Digital Citizen & Consumer Working Group (DCCWG). The DCCWG is a 13-member group that is studying the intersections between privacy/data protection and consumer protection/anti-trust as well as promoting cooperation between these regulatory spheres.
- The OPC attended and presented a regulatory update at the joint annual meeting of UCENet and the M3AAWG in Montreal in October 2019. The event was attended by anti-spam, consumer protection and telecommunications regulatory authorities and private-sector IT security experts.
- In May 2019 and December 2019, the OPC attended and participated in the 51st and 52nd Asia Pacific Privacy Authorities (APPA) Forums, in Tokyo, Japan and Cebu, Philippines, respectively.

Competition Bureau

Along with honouring foreign assistance requests, the Bureau continues to be active with a number of international and domestic partnerships and working groups. These include:

- the Organisation for Economic Co-operation and Development;
- the International Consumer Protection Enforcement Network;
- the International Mass Marketing Fraud Working Group;
- the Canadian Anti-Fraud Centre, Joint Management Team;
- the Toronto Strategic Partnership;
- the Alberta Partnership Against Cross-Border Fraud; and
- the Pacific Partnership Against Cross-Border Fraud.

5.4 Monitoring Compliance

Canadian Radio-television and Telecommunications Commission

The CRTC hosts the Spam Reporting Centre, which collects information that can serve as evidence of potential CASL violations.

In 2019–2020, Canadians made 309,985 submissions to the centre, up 10% from the previous year. Among these, 14,809 were submitted using the provided web form (up 71% from the previous year) and 295,176 were submitted as forwarded emails (up 8.2% from the previous year).

Submissions from Canadians are important—particularly when the web form is used, given that it collects detailed information. The CRTC uses this information to:

- analyze the data collected about complaints and perform regular environmental scans;
- identify trends and threats;
- initiate investigations; and
- take enforcement actions.

For example, agencies worldwide have seen a spike in scam activity related to the COVID-19 pandemic. In 2019–2020, CRTC staff worked to identify malicious sites associated with the emerging pandemic, and shared information with Government of Canada partners to disrupt and shut down these sites, helping to protect Canadians.

Competition Bureau

In April 2019, the Bureau's Deceptive Marketing Practices Directorate launched a Compliance Monitoring Unit. The unit was developed to ensure that matters that have been resolved through consent agreements, criminal sentencing orders, alternative case resolutions or other court orders are monitored more consistently to ensure compliance. The unit's compliance monitoring work also includes CASL-related matters resolved by the Bureau.

5.5 Enforcement

Canadian Radio-television and Telecommunications Commission

The CRTC is responsible for ensuring compliance with sections 6 through 9 of CASL. It has the power to investigate and take action against violators, and can set administrative monetary penalties.

In general, the CRTC's focus is on those who send commercial electronic messages without the recipient's consent or who install programs on computers or networks without consent. This includes malicious computer programs, spam messages and infected web links.

The CRTC publishes its enforcement actions In 2019–2020, these included:

- 202 Notices to Produce;
- 8 Preservation Demands;
- 6 Warning Letters; and
- 2 Notices of Violation (totalling $115,000 in AMPs).

In 2019–2020, the CRTC held an individual liable under CASL for the first time ever in connection with violations committed by a corporation pursuant to section 31 of CASL. Based on the evidence gathered, the CRTC found that nCrowd, Inc. sent emails without recipients' consent and without a properly functioning unsubscribe mechanism. Further, the CRTC found that Mr. Brian Conley, as president and CEO, allowed these violations to be committed. The CRTC imposed a $100,000 penalty on him.

Office of the Privacy Commissioner of Canada

CASL-related investigations

In 2019–2020, the OPC received 4 CASL-related complaints. Of these, 2 were closed at intake. The OPC is investigating the 2 remaining complaints.

During the year, the OPC:

- continued its industry-wide, commissioner-initiated investigation into the privacy management practices of data and list brokers (publication of the report is expected in 2020–2021);
- investigated an allegation about the covert installation of mobile device management software on an individual's cellphone (the allegation was withdrawn by the complainant after technical submissions received from the respondent enabled the Office to reassure him that the installation had not taken place);
- investigated an allegation concerning the covert installation of RAT software on an individual's laptop (ongoing); and
- investigated an allegation about the receipt of unsolicited email marketing (ongoing).

CASL-enabled investigations

CASL amended PIPEDA's provisions in 2011, enabling the OPC to collaborate and share information more easily with other provincial and international data protection authorities.

In 2019–2020, the OPC achieved a new high-water mark for information-sharing and collaboration with its domestic privacy enforcement counterparts when it began collaborating with the Office of the Information and Privacy Commissioner of Alberta (OIPC AB), the Office of the Information and Privacy Commissioner of British Columbia (OIPC BC) and the Commission d'accès à l'information du Québec (CAI) on matters of mutual interest and in several joint investigations:

- The OPC completed a joint investigation with the OIPC BC into the privacy practices of BC-based political consultancy firm **AggregateIQ** as part of the Facebook/Cambridge Analytica matter. The offices held a joint news conference and issued a joint report of findings in November 2019.
- The OPC continues to collaborate with the OIPC AB and OIPC BC in a joint investigation into **Cadillac Fairview's** use of facial recognition technology in mall digital directories.
- In July 2019, the OPC and the CAI announced parallel investigations into the privacy breach at **Desjardins** (ongoing).
- In February 2020, the OPC announced a joint investigation (with the OIPC AB, OIPC BC and the CAI) into **Clearview AI Inc.**'s collection and use of personal information without consent for the purposes of providing facial recognition information to law enforcement. This investigation remains active.

The past fiscal year also saw the OPC share information and cooperate with various international counterparts, including the UK Information Commissioner's Office, the US Federal Trade Commission, the Office of the Australian Information Commissioner, France's *Commission nationale de l'informatique et des libertés* and the Dutch Data Protection Authority on a range of compliance activities. This included several active and confidential OPC investigations with an international scope.

- In 2019–2020, the OPC and the UK Information Commissioner's Office also shared information and analysis arising from their respective investigations concerning AggregateIQ.

Competition Bureau

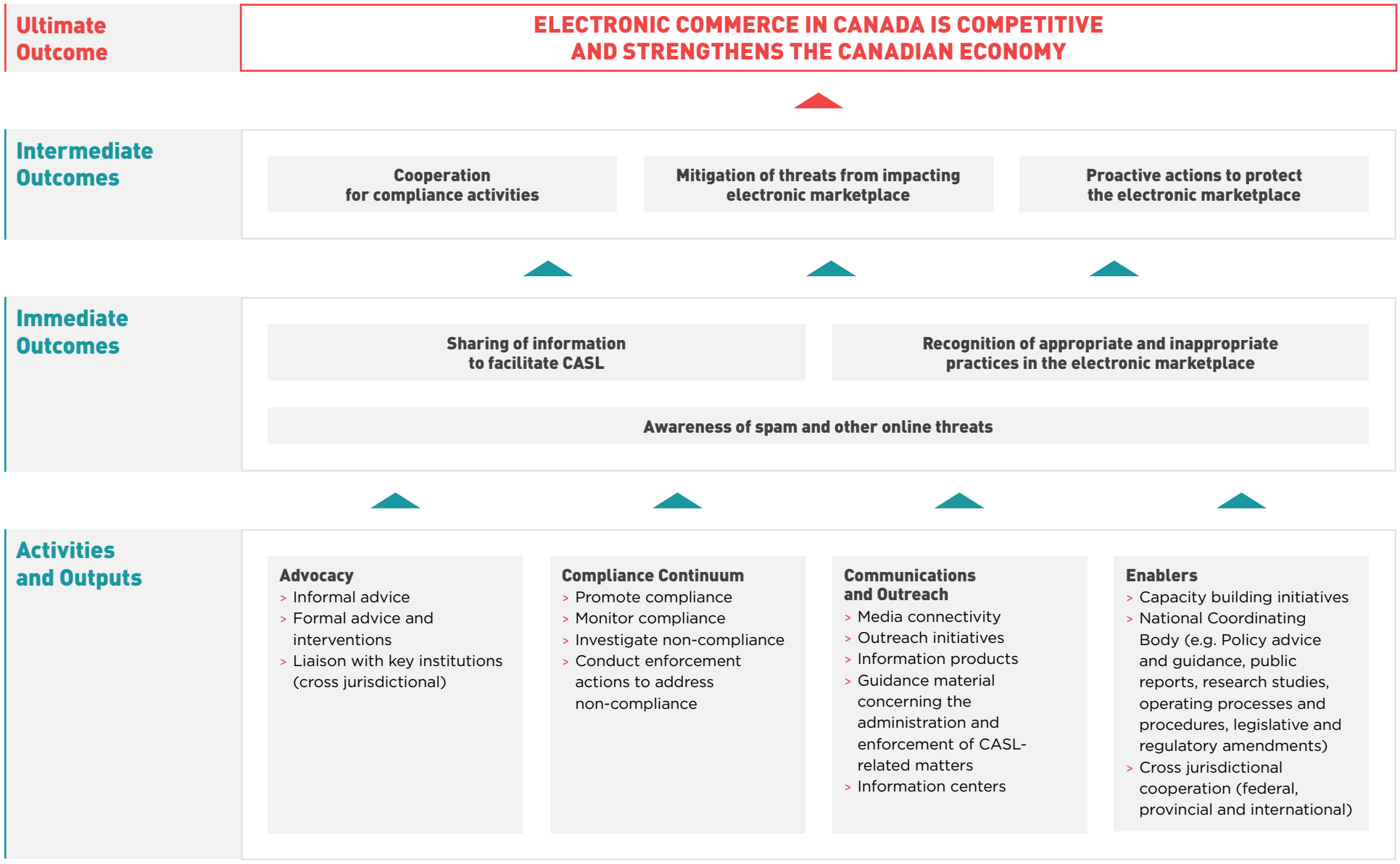
On June 27, 2019, the Bureau reached a consent agreement with Ticketmaster and related companies that resulted in a $4 million administrative monetary penalty as well as $500,000 to cover costs incurred by the Bureau during its investigation into alleged misleading pricing in online ticket sales.

On October 28, 2019, the Competition Bureau took action to protect consumers from false or misleading representations that result in hidden fees being charged for flights, while it continues its investigation into the marketing practices of FlightHub Group Inc. The Bureau entered into a temporary consent agreement with FlightHub that prohibits it from using false or misleading marketing practices on flighthub.com and justfly.com.

On February 13, 2020, the Bureau reached a consent agreement with Stub Hub that resulted in a $1.3 million AMP to correct what the Bureau concluded were misleading pricing claims in the online sale of tickets to entertainment and sporting events.

On March 11, 2020, the Bureau took legal action to stop NuvoCare and its president from making weight loss and fat-burning claims in the marketing of certain natural health products.

Annex A: CASL Logic Model



Description

The appendix shows a logic model for CASL. A logic model shows how program activities are expected to produce outputs and, in turn, how these outputs are expected to lead to different levels of results or outcomes.

There are 4 sets of activities and outputs:

1. Advocacy, including informal advice or correspondence, formal advice and interventions, and liaising with key institutions (cross-jurisdictional)
2. Compliance Continuum, including promoting compliance, monitoring compliance, investigating non-compliance, and conducting enforcement actions to address non-compliance
3. Communications and Outreach, including media connectivity, outreach initiatives, information products, guidance material concerning the administration and enforcement of CASL-related matters, and information centres
4. Enablers, including capacity-building initiatives, National Coordinating Body outputs (e.g., policy advice and guidance, public reports, research studies, operating processes and procedures, legislative and regulatory amendments) and cross-jurisdictional cooperation (federal, provincial and international)

The 4 sets of activities and outputs lead to 3 immediate outcomes:

1. Awareness of spam and other online threats
2. Sharing of information to facilitate CASL
3. Recognition of appropriate and inappropriate practices in the electronic marketplace

The 3 immediate outcomes lead to 3 intermediate outcomes:

1. Cooperation for compliance activities
2. Mitigation of threats impacting the electronic marketplace
3. Proactive actions to protect the electronic marketplace

The intermediate outcomes lead to one ultimate outcome: electronic commerce in Canada is competitive and strengthens the Canadian economy.