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

Canada

CANADA'S ANTI-SPAM LEGISLATION (CASL)

+

PERFORMANCE MEASUREMENT REPORT 2020-2021

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) annual performance measurement report aims to increase Canadians' general awareness of the CASL initiative. It provides relevant information about the initiative, its environment, its performance and its partners' roles and activities.

In an increasingly digital world, the purpose of CASL is to help Canada's economy be as efficient and adaptable as possible by regulating commercial conduct that could discourage consumers from doing business electronically. More precisely, it aims to protect Canadian businesses and consumers from spam, malware and other emerging electronic threats that:

- impair the availability, reliability, efficiency and optimal use of electronic means to carry out commercial activities;
- result in additional costs for businesses and consumers;
- compromise privacy or the security of confidential information; and
- undermine Canadians' confidence in the use of electronic platforms to carry out commercial activities at home and abroad.

CASL plays an important role in balancing the potential of a data-driven economy against Canadians' right to have their data and privacy protected. In a commercial context, CASL's rules prohibit, among other practices:

- spamming—sending commercial electronic messages without prior consent;
- deceptive marketing practices—making false and misleading claims online, including in website addresses;
- malware—installing software without prior consent;
- hacking—altering transmission data;
- address harvesting—using computers to collect electronic addresses without prior consent; and
- privacy invasions—using spyware and similar tools to collect or use individuals' personal information through unlawful access to their computer systems.

2. Partners

The CASL initiative engages multiple federal partners that have different but complementary mandates. As shown in the following diagram, Innovation, Science and Economic Development Canada (ISED), which includes the Office of Consumer Affairs (OCA), 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 and CASL-related provisions in other laws, including the *Personal Information Protection and Electronic Documents Act*, the *Competition Act* and the *Telecommunications Act*.

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, via any means of communication.
- encourages compliance with CASL-related PIPEDA provisions through outreach and remedies (excluding AMPs)

3. Results at a Glance

Promoting

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

In 2020–2021:

- The fightspam.gc.ca website received 148,464 visits.
- The CRTC's CASL-related website had 199,184 unique page views (up 17% from the previous year) and 238,250 page views (up 15% from the previous year).
- The OPC's CASL-related web pages were viewed more than 55,983 times.
- The Competition Bureau issued 2 CASL-related alerts to help consumers and businesses identify and avoid common scams.
- The Spam Reporting Centre received 285,505 submissions (representing approximately 7.5% fewer complaints than the previous year).
- The CASL enforcement partners collaborated on an awareness campaign and joint letter, contacting 36 companies from the mobile application industry to remind them of their CASL-related compliance obligations.

Enforcing

The agencies responsible for enforcing CASL and CASL-related provisions are the CRTC, the Competition Bureau and the OPC. These agencies have tools to respond to non-compliance, such as warning letters, notices of violation, undertakings and consent agreements. The CRTC can impose administrative monetary penalties (AMPs) and the Competition Bureau can seek AMPs through a court order or negotiated settlement, while the OPC can make recommendations, enter into compliance agreements with respondents, and seek court orders. These tools are meant to promote and enforce compliance with CASL and CASL-related regulations.

In 2020–2021, the CRTC issued:

- 1 decision;
- 1 undertaking with a payable amount of $100,000;
- 1 notice of violation with an AMP of $75,000;
- 400 notices to produce;
- 34 preservation demands; and
- 12 warning letters.

The Competition Bureau:

- resolved 1 matter through a guilty plea and 2 matters through a registered consent agreement with an AMP;
- acted in 1 matter to stop false or misleading advertising while it investigated; and
- sent more than 40 warning letters to sellers who were making potentially false or misleading claims related to the COVID-19 pandemic.

The OPC investigated:

- 1 allegation that remote access tool (RAT) software had been covertly installed on an individual's laptop by a computer services company (a report was issued); and
- 1 allegation of unsolicited email marketing against an insurance company (addressed through early resolution).

4. The Environment

4.1 International Context

Companies, governments and citizens around the globe are striving to keep up with the accelerating scale and pace of technological change. As outlined by the Canadian Centre for Cyber Security, technology is changing our societies and altering the threat landscape as the world becomes increasingly reliant on the internet. More and more important day-to-day activities, such as banking, government services, health services, commerce and education, have moved online for convenience and efficiency. In today's COVID-19 context, this trend has accelerated to allow citizens to work, shop and socialize remotely while respecting public health guidelines; however, this transition has also been marked by new tactics and opportunities from nefarious cyber actors.

When devices, information and activities move online, they become susceptible to threats. At the same time, the availability of cybercrime-as-a-service and ransomware-as-a-service on dark web marketplaces has diminished the barriers to entry for new nefarious actors, making it easier for them to carry out cyber attacks. They adapt their activities to find information of value, which they may attempt to obtain, hold for ransom or destroy.

Cyber threats do not respect national boundaries, and their ubiquity demonstrates how necessary it is for domestic and international law enforcers to cooperate to mitigate cybersecurity issues. It also demonstrates the vital role that private-public partnerships have to play in this area. To that end, CASL 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. CASL helps maintain a privacy and data protection framework that provides mechanisms to enhance interoperability domestically and internationally using privacy and e-protection laws.

4.2 Trends, Indicators and Challenges

Canada's cyber threat landscape is evolving, and cyber threat actors continue to adapt to keep up with the changing environment. As described above, the COVID-19 pandemic prompted these actors to innovate and find new ways to launch attacks. According to Europol's *Internet Organised Crime Threat Assessment 2020*, during the pandemic, violators devised new modi operandi and adapted existing ones to exploit the situation and target new victims. For example, these actors tweaked existing forms of cyber violations to fit the pandemic narrative and abused the uncertainty of the situation and the public's thirst for information. Pandemic-themed malicious emails, attachments, websites and even fake COVID-19 contact tracing apps were commonplace.

However, the opportunistic behaviour of malicious cyber actors during the pandemic should not overshadow the overall threat landscape. In many cases, the COVID-19 pandemic amplified existing security weaknesses, and these became more prominent and numerous when a significant number of people began to work from home. The year 2020 was record-breaking in terms of cyber attacks.

In 2020 in Canada:

- Most Canadians (87%) expressed concerns about privacy protections; 70% refused to provide an organization or business with their personal information due to privacy concerns; and 74% adjusted the privacy settings on a social media account.
- E-commerce became Canadians' main shopping outlet, and online stores became the most frequent targets of phishing attacks (18%).
- 40% of Canadians deleted a social media account due to privacy concerns or stopped doing business with a company that experienced a privacy breach.
- Organizations were less likely to inform a regulatory body of a data breach. Only 36% did so (versus 58% in 2019).
- Canadian organizations lost an estimated $5 billion to ransom payments and reduced productivity due to ransomware.

In 2020 worldwide:

- The share of spam in email traffic amounted to 50%, down 6% from 2019.
- 85% of all organizations were hit by a phishing attack at least once.
- 95% of all attacks targeting enterprise networks were caused by successful spear phishing.
- 30% of phishing emails were opened by users, and 12% of these targeted users clicked on the malicious link or attachment.
- About 1.5 million new phishing sites were created every month.
- The number of phishing emails that contained some form of ransomware rose to 97%.
- Eighty per cent of the spam received by internet users in North America and Europe can be traced to about 100 known spam operations listed in the Spamhaus Project's Register of Known Spam Operations database.
  - In 2020, none were Canadian, which means that most attacks targeting Canadians originate outside the country.
  - No operation originating in Canada figured in the Spamhaus database or on its 10 Worst Spammers list.
  - Canada did not figure on the Spamhaus 10 Worst Spam Countries list or 10 Worst Botnet Countries list.

5. The Results

5.1 Policy and Coordination

National Coordinating Body

The National Coordinating Body (NCB) keeps abreast of the most recent developments in spam, online threats, cybersecurity and e-commerce by performing strategic intelligence scans, conducting information research and analyzing metrics and trends. It also works with national and international partners to align legislative and regulatory frameworks with international anti-spam and malware industry best practices.

In 2020–2021, the NCB:

- helped develop the 2019–2020 CASL Performance Measurement Report, which was completed in collaboration with all CASL partners.
- participated in the Messaging, Malware and Mobile Anti-Abuse Working Group—a spam-related international forum—alongside Canadian partners.
- informed and advised ISED (the Department responsible for CASL) on all developments relating to CASL management and policy.
- coordinated CASL governance activities, such as the 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 CASL partners to increase awareness of the CASL initiative by coordinating communication, education and outreach activities.

5.2 Promoting Compliance

Office of Consumer Affairs

The OCA manages CASL-related communication products for Canadian individuals and businesses, including the CASL website, fightspam.gc.ca.

In 2020–2021, the OCA regularly updated the Spam news page at fightspam.gc.ca by linking to the latest reports and enforcement actions issued by CASL partners. The Office also conducted routine website maintenance, including updating content, fixing broken links and adding COVID-19 alert messaging.

Fightspam.gc.ca promotes CASL-related information. In 2020–2021, it received 148,464 visits.

Canadian Radio-television and Telecommunications Commission

Complementing fightspam.gc.ca, the CRTC's website also provides CASL-related information to Canadians and stakeholders to make it easier for everyone to get the help they need. The online experience includes easy-to-access alerts, videos, infographics, policies and guidelines to inform Canadians about CASL and help businesses comply. The CRTC also educates and informs stakeholders and Canadians through its social media platforms.

In 2020–2021, the CRTC:

- released 28 tweets (resulting in 5847 impressions) and 60 retweets;
- uploaded 12 Facebook posts, leading to 61,889 impressions and 19 reposts;
- released 12 LinkedIn publications that led to 8,232 impressions;
- conducted more than 24 stakeholder interactions through general outreach, video meetings, video partner briefings, video conference presentations and webinars;
- participated in weekly Twitter chats during Anti-Fraud Month (March) to raise awareness of fraud prevention methods for consumers and businesses;
- held a fireside chat with the CRTC's Chief Compliance and Enforcement Officer at the Canadian Email Summit;
- shared a presentation and exchanged ideas with the Canadian University Council of Chief Information Officers;
- published updates to the CRTC's guidance material relating to section 8 of CASL (requirements for installing computer programs);
- published 2 CRTC CASL Enforcement Dashboards on its website;
- released 2 case summaries in relation to a notice of violation and an undertaking;
- issued a news release announcing the outcome of a significant investigation into a hailstorm spam campaign (a hailstorm involves sending a high volume of emails out over a short time span before anti-spam defences can respond and block them); and
- updated the messaging on its website and social media to include scam-type activities related to the COVID-19 pandemic.

Given the restrictions caused by the COVID-19 pandemic, the CRTC's Compliance and Enforcement team engaged with companies, associations and organizations virtually to raise awareness about CASL's application to unsolicited communications.

In February 2021, the CRTC—along with its partners at the Canadian Anti-Fraud Centre, the Competition Bureau and the RCMP—participated in a weekly Twitter chat to raise awareness of fraud prevention methods for consumers and businesses alike.

Competition Bureau

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

In 2020–2021, the Bureau:

- issued 2 CASL-related alerts to help consumers and businesses identify and avoid non-delivery scams and common scams directed at businesses;
- released a general warning to industry against making false or misleading claims that their products and services could prevent, treat or cure COVID-19, calling on all businesses to review their marketing and labelling and act immediately to comply;
- issued 146 tweets, 90 Facebook posts and 60 LinkedIn posts to educate Canadians about deceptive marketing practices, warn them about online scams and encourage them to report deceptive practices and be vigilant when online;
- co-chaired Fraud Prevention Month with the RCMP and Canadian Anti-Fraud Centre to promote awareness of online fraud.

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 page about Canada's anti-spam legislation 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 and organizing an awareness campaign and letter to businesses; publishing and distributing educational material; and running radio spots across the country. Due to the pandemic, some outreach activities, such as exhibitions and in-person promotions, were on hold.

In 2020–2021, the OPC partnered with the 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 the harvesting of 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 Office also:

- published a new Privacy Guide for Businesses with a section on CASL;
- responded to 45 CASL-related inquiries from individuals and businesses, most often about consent.

5.3 International and Domestic Cooperation

Canadian Radio-television and Telecommunications Commission

Like its CASL partners, the CRTC has forged partnerships with organizations across the globe to better fulfill its mandate. The Commission continues to belong to the Unsolicited Communications Enforcement Network (UCENet). UCENet members come from more than 26 countries. They work together to promote cooperation on spam enforcement internationally and address problems related to spam and unsolicited telecommunications.

In 2020–2021, the CRTC joined forces with the OPC and the Competition Bureau in the first joint CASL-related compliance initiative. The enforcement partners issued letters to 36 companies involved in the mobile app industry in Canada reminding them of their obligations under federal legislation. The letters emphasized that companies offering apps must ensure their products are CASL-compliant. This initiative also included an awareness campaign geared toward consumers that reached about 77,500 people through traditional media and 40,918 through social media, with 2,238 website hits received.

This initiative raised concerns around:

- apps that make false or misleading claims to promote a product, service or business interest;
- apps that collect or use personal information, such as "keylogging" malware, without consent;
- apps that do not completely identify their functions as part of obtaining informed consent from the user prior to installation; and
- apps designed to spam users' friends and contacts.

These activities put Canadians at risk of fraud, identity theft and financial loss, among other problems. The 36 companies are in a unique position to detect, prevent and stop such practices from harming consumers.

Finally, the letter encouraged the businesses to review their practices and take preventive and corrective measures where needed.

Competition Bureau

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

- Organisation for Economic Cooperation and Development
- Global Anti-Fraud Enforcement Network, formerly known as the International Mass Marketing Fraud Working Group
- Canadian Anti-Fraud Centre, Joint Management Team
- Toronto Strategic Partnership
- Alberta Partnership Against Cross-Border Fraud
- Pacific Partnership Against Cross-Border Fraud
- International Consumer Protection Enforcement Network (ICPEN)

ICPEN is a network of consumer protection and law enforcement authorities from more than 65 countries whose objective is to protect consumers by encouraging global cooperation among law enforcement agencies and the sharing of information about cross-border challenges that affect consumers.

On July 1, 2020, the Bureau began a 1-year term as ICPEN president. During that year, the Bureau and other ICPEN members explored ways to deter deceptive marketing with a focus on the following themes:

- examining global best practices around remote investigative and consumer protection work to better adapt to misleading and fraudulent marketing activities related to the COVID-19 pandemic;
- exploring the pros and cons of artificial intelligence (AI), which can be both a powerful investigative tool and an opportunity for businesses to mislead consumers;
- looking at enforcement challenges, data privacy concerns and third-party responsibilities associated with digital platforms;
- examining ways to address misleading activities that attempt to exploit consumers' concerns about the environment.

As well, as ICPEN president, the Bureau hosted a series of 4 best practices webinars in February 2021. One of these was held in collaboration with the OPC through the Global Privacy Enforcement Network (GPEN) and was devoted to the topic of consumer data privacy.

Office of the Privacy Commissioner of Canada

Throughout 2020–21, CASL enforcement partners worked with their domestic and international counterparts to promote compliance with the legislation. Given the internet's borderless nature, CASL violations can originate outside Canada. As such, international cooperation is often needed to investigate online threats. Information-sharing and cooperation with foreign governments and organizations are essential to ensure effective and coherent global actions against CASL violators.

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 by participating in regulatory networks. In fact, such cooperation has now become the normal course of business. This fact is highlighted by the numerous collaborative investigations that were launched or completed in the past year (see Section 5.5, Enforcement, Office of the Privacy Commissioner).

The OPC is a member of the executive committee of GPEN. As such, it participates in collaborative enforcement activities, hosts and administers the GPEN website, and takes part in monthly calls and network meetings about privacy.

- In March 2021, GPEN members (including the OPC) worked with ICPEN to hold the first-ever joint best practices workshop. The virtual event brought together international enforcement practitioners from both regulatory spheres to discuss the substantive intersection between privacy and consumer protection and explore strategies to advance practical cross-regulatory enforcement cooperation.
- The first-ever collaborative activity between GPEN and ICPEN, whereby GPEN endorsed a letter from 27 ICPEN agencies to both Apple and Google, generated results in 2020–21, with both companies introducing changes to enhance the information that apps provide to users about how their data are being collected and used.
- In response to the COVID-19 pandemic, GPEN conducted a virtual discussion and subsequent survey to gauge the impact of the pandemic on the operations of data protection authorities and to share approaches for enforcement during and as we emerge from the pandemic.

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 around the world.

- In October 2020, the OPC attended and presented at the virtual 42nd GPA conference.
- The OPC is also co-chair of the GPA's International Enforcement Collaboration Working Group (IEWG), whose members are advancing cooperation on privacy enforcement across international jurisdictions and establishing practical measures to support this. In 2020–2021, the IEWG facilitated several virtual meetings among privacy authorities to discuss and share perspectives on issues such as COVID-19 tracing apps, facial recognition technology and credential stuffing (a common form of cyber attack).
- In July 2020, the OPC and 5 other GPA members—brought together through the IEWG—published a joint statement on the global privacy expectations of video teleconferencing companies. While intended for all such companies, the letter was sent directly to 5 of them. Four replied to describe the steps they had taken to comply with data protection and privacy requirements. The joint signatories issued an updated statement in December 2020, and will further engage with each of these companies to better understand their platforms and privacy practices in 2021–2022.
- The OPC also co-chairs the GPA's 13-member Digital Citizen & Consumer Working Group, which is studying the intersections between privacy/data protection and consumer protection/anti-trust as well as promoting cooperation between these regulatory spheres. In 2020–2021, the group gave a presentation and facilitated breakout sessions at the first-ever joint ICPEN/GPEN Best Practices Workshop. It also conducted competition regulator interviews to gain insights into the intersection of privacy and competition regulation and commissioned an independent academic review of this intersection.

The OPC is a member of UCENet. UCENet did not hold an annual meeting in 2020, but the OPC participated in member calls and attended the virtual annual meeting of the Messaging, Malware and Mobile Anti-Abuse Working Group in October. The event was also attended by anti-spam, consumer protection and telecommunications regulatory authorities and IT security experts.

In June 2020 and December 2020, the OPC participated in the 53rd and 54th Asia Pacific Privacy Authorities Forums. The 53rd forum examined and discussed privacy challenges presented by the COVID-19 pandemic, biometric information and data breach notification issues. The 54th forum continued to examine the privacy implications of the pandemic, and discussed facial recognition technology, AI and the future of privacy frameworks.

Finally, at a September 2020 COVID-19 webinar organized by the authorities, the OPC presented its techniques to leverage virtual tools and continue collaborating with other agencies through the IEWG during the pandemic.

5.4 Monitoring Compliance

Canadian Radio-television and Telecommunications Commission

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

In 2020–2021:

- Canadians made 285,505 submissions to the centre (down 7.5% from last year).
- 8,413 of these submissions arrived through web form submissions, and 277,092 were forwarded through email.

Submissions from Canadians are important—particularly web form submissions, in which the information provided tends to be more detailed. The CRTC uses this information to:

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

For example, by analyzing data from the SRC, the CRTC was able to detect a hailstorm spam campaign in which an individual was sending out a high volume of emails over a short time span, before anti-spam defences could respond and block the messages.

Competition Bureau

The Compliance Monitoring Unit of the Competition Bureau's Deceptive Marketing Practices Directorate monitors matters—including CASL-related matters—that have been resolved through consent agreements, criminal sentencing orders, alternative case resolutions or other court orders.

Office of the Privacy Commissioner

The OPC's Compliance Monitoring Unit continues to engage with organizations to ensure they honour the commitments they have made to the Office and implement satisfactory measures to address the OPC recommendations that flow from reports of findings and compliance agreements.

5.5 Enforcement

Canadian Radio-television and Telecommunications Commission

The CRTC is responsible for ensuring compliance with sections 6 through 9 of CASL. The Commission has the power to investigate and act against violators and can set AMPs.

In general, the CRTC focuses 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. As mentioned in Section 3, Results at a Glance, in 2020–2021, these included:

- 1 decision;
- 1 undertaking with a payable amount of $100,000;
- 1 notice of violation with an AMP of $75,000;
- 400 notices to produce;
- 34 preservation demands; and
- 12 warning letters.

In June 2020, the CRTC issued Compliance and Enforcement Decision CRTC 2020-196, which upheld a requirement for Hydro-Québec to produce information related to 10 service addresses and their associated customer accounts.

In September 2020, the CRTC issued an undertaking that included a monetary payment of $100,000 and the implementation of a compliance program for alleged violations of CASL. The CRTC reached an agreement with Notesolution Inc. (doing business as OneClass) to resolve the alleged violations. OneClass agreed to make a payment of $100,000 and to develop and implement a CASL compliance program.

In March 2021, the CRTC issued the largest penalty under CASL to an individual to date. Based on information gathered over the course of the investigation, the Chief Compliance & Enforcement Officer issued a notice of violation, including an AMP of $75,000, to Scott William Brewer for sending commercial electronic messages without recipients' consent.

Competition Bureau

The Competition Bureau is responsible for enforcing the *Competition Act* and investigating cases that relate to false or misleading electronic representations and deceptive marketing practices in the electronic marketplace.

As mentioned briefly in Section 3, Results at a Glance, in 2020–2021, the Bureau:

- resolved 1 matter through a guilty plea and 2 matters through Registered Consent Agreements with an AMP;
- acted in 1 matter to stop false or misleading advertising while it investigated; and
- sent more than 40 warning letters to sellers who were making potentially false or misleading COVID-19-related claims.

On May 13, 2020, following legal action by the Bureau, NuvoCare Health Sciences and its President and CEO, Ryan Foley, agreed to enter into a temporary consent agreement prohibiting the company from making unsubstantiated weight loss and fat-burning claims when marketing certain natural health products, including WeightOFF Max! and Forskolin NX.

On May 19, 2020, the Bureau reached an agreement with Facebook concerning its conclusion relating to false or misleading claims about the privacy of Canadians' personal information on Facebook and Messenger. The agreement included a $9 million AMP.

On January 28, 2021, following legal action by the Bureau, a Canadian company doing business as Revive You Media (1806369 Alberta Limited) pleaded guilty in the Provincial Court of Ontario to an accusation of promoting deceptive free trial offers for health and dietary supplements that trapped consumers into monthly subscriptions. The plea resulted in $15 million in fines.

On February 24, 2021, the Bureau registered a consent agreement with the operator of FlightHub.com and JustFly.com to resolve the Bureau's concerns about marketing practices. The Bureau concluded that the online travel agencies charged hidden fees, authored positive customer reviews to promote their services, and made numerous false or misleading claims about prices and services. This resulted in a $5 million AMP for FlightHub Group Inc. and a $400,000 AMP for each of its 2 directors, Matthew Keezer and Nicholas Hart.

Finally, the Bureau has issued more than 40 warning letters to sellers who have made unsubstantiated or potentially false or misleading claims related to COVID-19. The warnings concerned claims related to masks, food and natural products, ventilation and air purification products, and more. Most of the businesses have taken corrective action, pulling products that raised concerns from their shelves or stopping the claims.

Office of the Privacy Commissioner

In 2020–2021, the OPC received 2 new potential CASL-related complaints. Of these, 1 was closed at intake due to a lack of jurisdiction, and the other was handled through early resolution.

As mentioned briefly in Section 3, Results at a Glance, the OPC also completed investigations related to:

- 1 allegation that RAT software had been covertly installed on an individual's laptop by a computer services company (a report was issued); and
- 1 allegation about the receipt of unsolicited email marketing from an insurance company (resolved through early resolution).

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 on compliance and enforcement-related matters.

Despite the impact of the pandemic throughout 2020–2021, the OPC expanded its information-sharing and collaboration efforts with its domestic privacy enforcement counterparts. The Office continued to work 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), the Commission d'accès à l'information du Québec (CAI), and the Office of the Information and Privacy Commissioner of Ontario (IPC) on matters of mutual interest, including an unprecedented number of joint investigations:

- In June 2020, the OPC, along with the OIPC AB, OIPC BC and the CAI, launched a joint investigation into a Tim Hortons' mobile application after media reports raised concerns about how the app might be collecting and using data about people's movements as they went about their daily activities. At the end of the fiscal year, this investigation was ongoing.
- In October 2020, the OPC, OIPC BC and OIPC AB released their findings in the matter of Cadillac Fairview's use of embedded cameras in its shopping mall digital information kiosks. The cameras collected 5 million shoppers' images and used facial recognition technology to guess their age and gender.
- In December 2020, the OPC, along with its counterparts at the CAI in Québec, published the findings of separate but coordinated investigations into a major privacy breach at Desjardins.
- In February 2021, with the OIPC AB, OIPC BC and the CAI, the OPC announced the findings of a joint investigation into Clearview AI's facial recognition app. This was the first investigation completed jointly with all 3 provinces under their respective private-sector privacy laws.
- Finally, in March 2021, the OPC issued its findings on the safeguards, breach reporting and notification, and accountability practices of CoreFour Inc. pertaining to Edsby, its K–12 education software application. During the investigation, the OPC shared information with the IPC, which conducted a separate but complementary investigation into a provincial school board that had adopted Edsby.

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 and the Office of the Australian Information Commissioner—on a range of compliance activities. These included active and confidential OPC investigations that were international in scope.

Summary

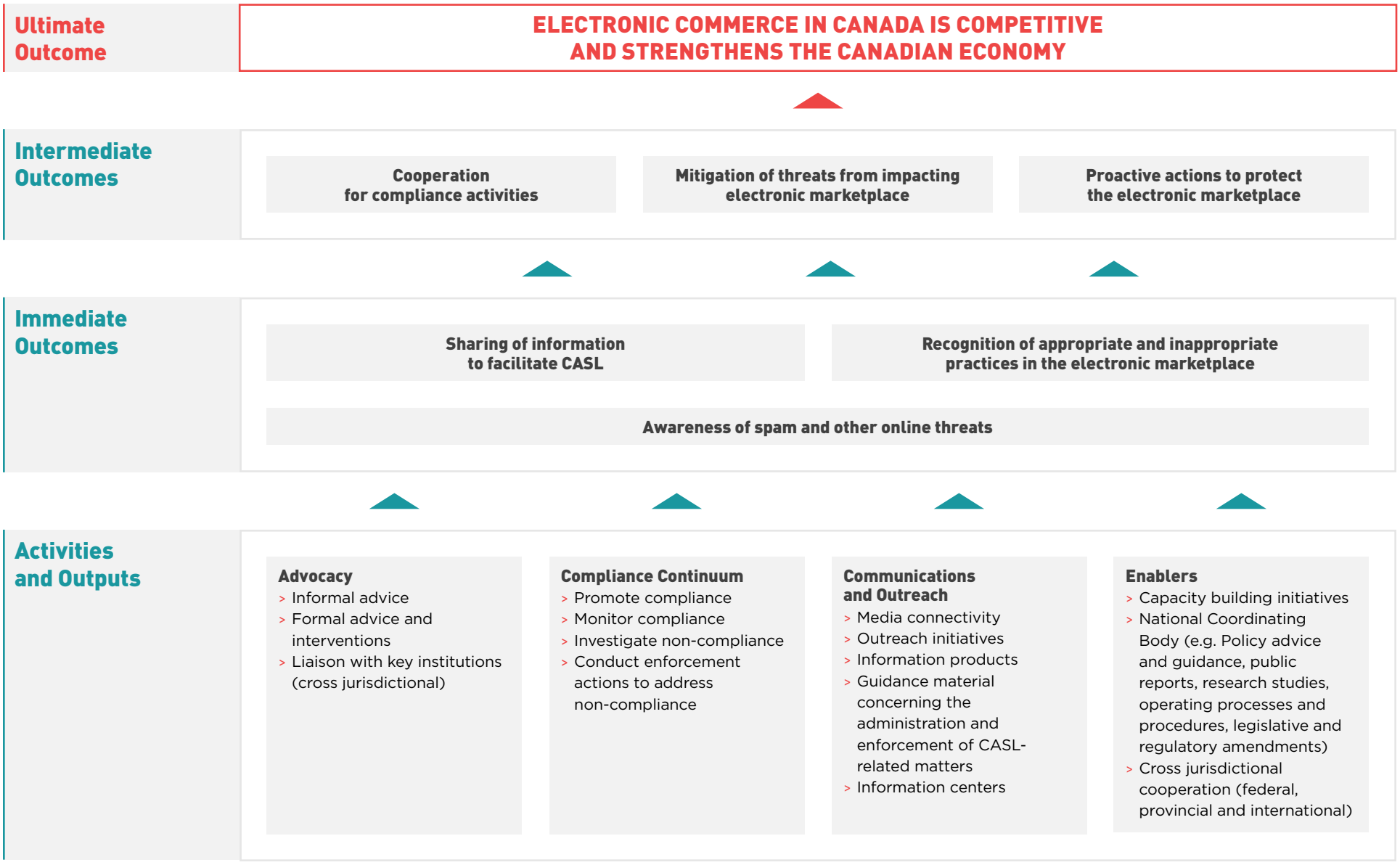
In a ever evolving cyber threat landscape, CASL continues to help protect Canadians from spam and other electronic threats that lead to harassment, identity theft and fraud, while ensuring that businesses can continue to compete in the global marketplace by establishing rules consistent with international best practices and anti-spam legislations.

The year 2020 was record-breaking in terms of cyber attacks. In many cases, the COVID-19 pandemic amplified existing security weaknesses, and cyber threats became more prominent and numerous as people transitioned to remote work. In addition, the advent of cybercrime-as-a-service has diminished entry barriers for new nefarious actors, making it easier for them to carry out cyber attacks. The ubiquity of cyber threats demonstrates how necessary it is for domestic and international authorities to cooperate to mitigate cybersecurity issues, which CASL partners have continuously been doing successfully.

In 2020-21, CASL partners continued to ensure the effectiveness of the CASL regime in addressing spam, malware, deceptive marketing practices, hacking, address harvesting and privacy invasions online. The CASL partners undertook numerous unilateral and collaborative actions to promote CASL awareness and compliance. They also continued to forge partnerships with organizations across the globe to better fulfill their respective mandate.

This performance report underlines the results of the efforts of the CASL partners. Great strides have been made in 2020-21 and the CASL partners will continue building an even more efficient CASL initiative.

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 a**ctions to protect the electronic marketplace**

The intermediate outcomes lead to 1 ultimate outcome: electronic commerce in Canada is competitive and strengthens the Canadian economy.