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

CANADA'S ANTI-SPAM LEGISLATION (CASL)

+ PERFORMANCE MEASUREMENT REPORT 2021-2022

This publication is available online at:
https://ised-isde.canada.ca/site/canada-anti-spam-legislation/en/canadas-anti-spam-legislation-resources/performance-measurement-reports/canadas-anti-spam-legislation-casl-performance-measurement-report-2021-22

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

This annual performance measurement report focuses on Canada's anti-spam legislation (CASL), and is the result of a collaboration between the following partners:

- the Canadian Radio-television and Telecommunications Commission (CRTC)
- the Office of the Privacy Commissioner of Canada (OPC)
- the Competition Bureau
- Innovation, Science and Economic Development Canada (ISED), which includes the Office of Consumer Affairs (OCA)

The report aims to increase awareness of the legislation among Canadian businesses and consumers by giving them information about CASL, its environment, its effectiveness, and the roles and activities of the organizations that help enforce it.

In this report, the term CASL encompasses the initiative, the legislation and its amendments to legal frameworks in the fields of telecommunications, competition and privacy; and in relation to cybersecurity and e-commerce.

CASL works to ensure that Canadian businesses can compete in the global marketplace. It does this by establishing rules that are consistent with international best practices and anti-spam legislation while remaining fair to organizations that strive to comply with the legislation. The legislation has a positive impact on consumer confidence because it regulates practices that could discourage them from doing business digitally. This strengthens the Canadian economy and makes it more adaptable in the face of a continuously evolving e-commerce context.

CASL's rules prohibit:

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

2. Partners

As shown in the following diagram, the CASL initiative engages multiple federal partners through different but complementary mandates.

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 telecommunication.
- encourages compliance with CASL-related PIPEDA provisions through outreach and remedies (excluding AMPs)

3. Context and trends

In 2004, unsolicited commercial electronic messages, known as spam, were a considerable global challenge, accounting for as much as 80% of global email traffic. In addition to spam, other electronic threats—such as identity theft, phishing, false and misleading content and malware—started to spread and disrupt productivity. This increase in electronic threats prompted the Canadian government to organize a multi-stakeholder Anti-Spam Task Force.

In 2005, the task force report expressed the need for a standalone, technology-neutral law to address spam, spam-related activities, and emerging electronic threats. This recommendation laid the foundation for CASL, which was enacted in 2010. Most of CASL's provisions came into force in 2014, with a 3-year transition period to build awareness of the new provisions and give businesses time to comply.

Today, CASL is part of a broad range of domestic and international legal and policy frameworks related to telecommunications and cybersecurity. Its regulatory framework supports e-commerce best practices and interoperability domestically and internationally with anti-spam, e-privacy and data protection regulatory frameworks.

Trends

Many cybersecurity trends from 2020 carried over into fiscal year 2021–2022:

- Spam remained a global problem, making up 45% of all email communications
- The COVID-19 pandemic amplified existing security weaknesses and forced businesses to navigate them in real time
- Cyber threats became more prominent and numerous as people continued to work remotely
- 36% of Canadian organizations indicated that they faced more cyber attacks during the pandemic (up from 29% in 2020)
- Worldwide, ransomware breaches increased by 13% (a 1-year increase that exceeded the rate of increase over the past 5 years combined)
- Cybercrime-as-a-service made it easier to carry out cyber attacks
- Roughly 4 in 5 breaches were attributed to organized crime
- Ransomware continued to prove particularly damaging for its ability to exploit and monetize illegal access to private information
- Heightened geopolitical tensions increased the sophistication, visibility and awareness of cyber attacks from nation states
- Canadian organizations became more concerned about potential harm from future cyber attacks, with 61% of organizations expressing concerns about this (versus 54% the previous year)
- The most common impacts of cyber attacks for organization were:

    - tying up employees' time and/or preventing them from working
    - reputational damage (reported by 19% of respondents, up from 6% in 2018)
    - loss of revenue (18%)
    - data breach/exfiltration associated with malware such as botnets and ransomware (17%)
    - loss of customers (13%)
    - reluctance to carry out planned activities (13%)

Against this challenging backdrop, with the CASL initiative, Canada is working hard to stop spammers from operating within its borders. Its efforts seem to be paying off:

- Up to 80% of spam targeted at internet users around the world is generated by around 100 spammers listed in the Spamhaus Project's Register Of Known Spam Operations database, and there is no Canadian organization on the Spamhaus 10 Worst Spammers list
- Canada does not figure in the Spamhaus list of the 10 Worst Spam Countries
- Canada does not appear in the Spamhaus list of the 10 Worst Botnet Countries, which tallies the countries with the highest number of detected spam-bots (most bots can be used for spam, phishing, click-fraud, distributed denial-of-service and other malicious activities)

The ubiquity of cyber threats underscores how necessary it is for domestic and international authorities to cooperate to mitigate cybersecurity issues.

Since November 2018, the Personal Information Protection and Electronic Documents Act (PIPEDA) has required private sector organizations subject to the act to report all breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals. In 2021–2022, the OPC received 645 reports of breaches affecting at least 1.9 million Canadian accounts, including online accounts (email, social media, websites, mobile apps) and others (bank accounts, credit cards, mobile phones or insurance policies).

The leading causes involved unauthorized access, with 419 reported incidents (65%). These incidents often arose when external bad actors accessed corporate systems. Among these incidents, 290 (69%) were considered to be cyber incidents, meaning they involved the use of malware, ransomware, hacking or phishing.

4. Results

4.1 Setting policy and ensuring coordination National Coordinating Body

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 industry best practices for handling international anti-spam and malware.

As part of ISED's Privacy and Data Protection Directorate, the NCB is responsible for setting policy, conducting oversight, and monitoring and reporting on the overall effectiveness of CASL. The NCB achieves these goals by:

- assessing the need for legislative, regulatory and policy improvement
- monitoring domestic and international developments
- undertaking research and consulting with public and private sector stakeholders in Canada and internationally
- collaborating with CASL partners to promote awareness and educate consumers and businesses
- facilitating the legislative process and working to enhance public and stakeholder understanding
- participating in international discussions related to spam, online threats, cybersecurity and e-commerce

In 2021–2022, the NCB:

- helped develop the 2020–2021 CASL Performance Measurement Report in collaboration with 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 of 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 CASL website
- collaborated with CASL partners to increase awareness of the CASL initiative by coordinating communication, education and outreach activities

4.2 Promoting compliance

Office of Consumer Affairs

The OCA promotes compliance with CASL by running education and awareness initiatives. It manages CASL-related communications products, including the CASL website, fightspam.gc.ca, which presents CASL-related information for the consumer and business audiences. In 2021–2022, the website received 79,908 visits from the following countries:

- 51% from Canada
- 28% from the United States
- 11% from the United Kingdom
- 10% from all other countries

Spam targeting Canadians (whether through commercial electronic messages, malware, software or altered transmission of data) is subject to CASL no matter the country of provenance. Consequently, the legislation and the CASL website are of interest to anyone wishing to engage in sending commercial electronic messages to or from Canada.

The OCA regularly updated the website's Spam news page by linking to the latest reports and enforcement actions issued by its CASL partners. It also refreshed content, fixed broken links and updated its COVID-19 messaging.

The OCA creates CASL-related communications products and promotes them through social media. In December 2021, its tweets and Facebook posts helped businesses ensure their holiday messages to consumers complied with CASL. Tweets through the English and French ISED channels reached 1,871 users.

The OCA monitors online news sources and social media to track sentiment toward CASL. In 2021–2022, media monitoring captured 6,259 CASL-related mentions, and sharing resulted in 171,000 amplifications. Out of these mentions:

- 56% were positive
- 17% were neutral or ambivalent
- 27% were negative

There was a 6% increase from the previous year in mentions that had a positive tone. However, there was also an increase in negative sentiment.

Key media coverage trends

- Most social media posts focused on the benefits of CASL and involved professionals offering insights or expertise
- Most tweets were from technology professionals offering opinions on how companies should implement CASL and/or monitor their adherence to it
- Tweets expressing confidence in and praise for CASL often increased in volume after announcements of enforcement actions
- The tone of negative posts suggested concern that certain companies or political parties were not complying with the legislation, with many calling for punitive action
- Ransomware and malware garnered the highest number of mentions, with spam and privacy concerns cited less frequently
- In terms of spam (22% of media reports) and abuse of electronic means of communication (8% of media reports), most posts mentioned scams, robo calls and text messages

Canadian Radio-television and Telecommunications Commission

In 2021–2022, the CRTC used a variety of approaches to promote compliance with CASL. These included stakeholder interactions, information sharing, video meetings, video partner briefings, video conference presentations, webinars, and an informal fireside chat with the CRTC's Chief Compliance and Enforcement Officer.

The CRTC promoted CASL compliance among businesses doing e-commerce in Canada by posting 3 new educational videos to its YouTube playlist with tips on how to comply with Canada's marketing rules (for an example, see Spam and Telemarketing – Stir in the regulations). It also issued 2 news releases to encourage businesses to comply with CASL and highlight the penalties for non-compliance.

In addition, the CRTC continued to raise awareness of CASL among Canadians. Some highlights include:

- publishing 2 biannual snapshots of CASL enforcement activities
- creating an easy-to-follow infographic about how to spot an online scam
- issuing social media alerts about investment scams, including those involving cryptocurrency payments
- promoting the CASL email address and the Spam Reporting Centre's (SRC's) online form across multiple social media platforms

Competition Bureau

The Bureau increases awareness of CASL-related issues in a variety of ways to reach as many Canadian consumers and businesses as possible. In 2021–2022:

- The Bureau ran Fraud Prevention Month, an tannual event that helps consumers and businesses recognize, reject and report fraud
  - This year's theme was impersonation scams

- Throughout Fraud Prevention Month, the Bureau published a consumer alert about fake reviews (entitled Five-star fake out) and issued social media posts on this and related topics, such as third-party seller fraud, fake or cloned websites, and business fraud
- The Bureau issued a new consumer alert about greenwashing to educate consumers about this practice and help them recognize it
- The Bureau updated a page on its website about representations in electronic messages and web addresses and published a new web page about environmental claims and greenwashing

Office of the Privacy Commissioner of Canada

The OPC publishes CASL-related compliance guidance for businesses and advice for individuals on various channels. Although it carries out CASL-related outreach activities throughout the year, the CASL page on its website is its primary tool for sharing information.

In 2021–2022, the OPC:

- received 31,077 unique page views of its CASL-related web pages
- responded to 51 CASL-related calls, inquiries and submissions from individuals and businesses
- published 92 tweets and 24 LinkedIn posts about CASL that resulted in some 138,000 impressions
- updated 2 web pages (Be diligent when dealing with spam and Proceed with caution: Avoid malicious software) to encourage individuals to report fraud and spam using the SRC's online form
- launched a radio campaign on ways to identify spam that aired on local stations in Canada from December 6, 2021 to January ran 26, 2022, reaching more than 1.8 million listeners

4.3 Cooperating across Canada and internationally

Canadian Radio-television and Telecommunications Commission

In 2021–2022, the CRTC continued to forge partnerships with organizations across the globe to strengthen ongoing efforts to combat spam. For instance, the commission renewed its memorandum of understanding with the Australian Communications and Media Authority. The memorandum leverages a strong relationship to share strategic approaches, exchange intelligence and provide mutual assistance with investigations.

Competition Bureau

Along with honouring requests for assistance from other countries, the Bureau continued to participate in a number of international and domestic partnerships and working groups, including with the:

- Organisation for Economic Cooperation and Development
- International Consumer Protection Enforcement Network
- Global Anti-Fraud Enforcement Network
- Canadian Anti-Fraud Centre Joint Management Team
- Toronto Strategic Partnership
- Alberta Partnership Against Cross-Border Fraud
- Pacific Partnership Against Cross-Border Fraud

Office of the Privacy Commissioner of Canada

The OPC is a member of several organizations that are concerned with privacy and data protection online, including:

- the Global Privacy Assembly, which connects more than 130 data protection and privacy authorities from around the world and fosters international collaboration
- the executive committee of the Global Privacy Enforcement Network, where the OPC participates in enforcement activities, network website administration and privacy discussions
- the Unsolicited Communications Enforcement Network, where the OPC participates in discussions and presents regulatory updates

The OPC also chairs or participates in assembly working groups, including the International Enforcement Cooperation Working Group (IEWG) and the Digital Citizen and Consumer Working Group (DCCWG):

- The IEWG fosters cooperation on critical global privacy issues. In 2021–2022, it held virtual discussions on topics like facial recognition technology, credential stuffing, data-scraping and the AdTech ecosystem, all of which the OPC contributed to. ("AdTech" is short for advertising technology and refers to the technologies, software and services used to buy, sell, serve, track and analyze digital ads and campaigns.)
- In October 2021, the OPC and 5 of its IEWG counterparts published their observations about the global privacy expectations of video teleconferencing companies. The text outlines what good privacy practices exist and where there may be opportunities to improve.
- The DCCWG studies the intersections between privacy and other regulatory spheres, including competition and consumer protection, and promotes cross-regulatory cooperation. In October 2021, it issued a report (with the OPC as the lead author) that identified opportunities for better cross-regulatory collaboration.

In June 2021 and December 2021, the OPC participated in the 55th and 56th Asia Pacific Privacy Authorities forums:

- At the 55th forum, the OPC presented on recent law reform developments in Canada and data breach notifications
- At the 56th forum, the OPC spoke on vaccine-related developments and activities in Canada, identity-based harm in the digital environment, and the de-identification of personal data

Finally, in March 2022, the OPC entered into a renewed and updated information-sharing memorandum of understanding with the Netherlands' data protection authority.

Domestic cooperation

Federal, provincial and territorial information and privacy commissioners meet annually to coordinate on matters of public policy and education, and they sometimes issue calls for action that encourage consistent privacy protection for Canadians. The OPC liaises with its domestic counterparts through the Private Sector Privacy Forum and the Domestic Enforcement Collaboration Forum, which include representatives from the OPC, Alberta, British Columbia and Québec.

In December 2021, the OPC entered into a new information-sharing memorandum of understanding with the Office of the Information and Privacy Commissioner of Nunavut. In March 2022, it renewed and expanded a longstanding memorandum of understanding with the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia to include the Commission d'accès à l'information du Québec (CAI).

4.4 Monitoring compliance

Canadian Radio-television and Telecommunications Commission

The CRTC hosts the SRC, which collects information that can serve as evidence of potential CASL violations. In 2021–2022, Canadians submitted 322,345 spam reports to the centre—an increase of 12.9% from the previous year.

But the SRC doesn't only allow Canadians to report spam. It also gives the 3 enforcement agencies responsible for ensuring compliance with CASL access to a central database to use for investigative and enforcement purposes. In 2021–2022, the CRTC developed and made significant enhancements to the search and reporting functions in the SRC case management system. For example, the SRC now also includes:

- a PDF document analysis function that facilitates meta data and content processing
- sub-categories to better specify and triage complaints
- a section where users can provide additional information about complaints

These improvements will support more complex searches and allow the CRTC and enforcement agencies to create a variety of analytical reports to help identify trends, violations, and areas for investigation.

Competition Bureau

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

Office of the Privacy Commissioner

The OPC engages with organizations to ensure they honour their commitments and address the OPC recommendations that flow from reports of findings and compliance agreements.

In 2021–2022, the office upgraded its technology laboratory to expand its size and range. With dedicated work areas for different technologies, the additional workspace allows more employees to perform analyses. As a result, the OPC can now better monitor technological privacy risks. The office's connectivity to the SRC was reduced while these changes were being made, but it is now better equipped to monitor compliance going forward.

4.5 Enforcing CASL

Canadian Radio-television and Telecommunications Commission

The details of CRTC investigations associated with violations of sections 6 through 9 of CASL—and any resulting administrative monetary penalties (AMPs) —are published on the CRTC's Enforcement actions web page.

In 2021–2022, the CRTC led investigations that resulted in a total of $327,500 in AMPs. In addition:

- Its enforcement actions included 542 Notices to Produce, 43 Preservation Demands, 1 Search and 2 Undertakings
- An investigation targeting Dark Web marketplace vendors resulted in AMPs totalling $300,000
- Gap Inc. agreed to pay $200,000 for allegedly violating Canada's anti-spam legislation

Competition Bureau

In July 2022, the Competition Bureau made progress on 2 ongoing investigations into potentially false or misleading representations made in electronic messages or web addresses:

- The Bureau obtained a court order to advance an ongoing investigation into claims made by NuvoCare Health Sciences Inc. about certain natural health products, including WeightOFF Max! Forskolin+ and Forskolin Nx
- The Bureau obtained a court order to advance an ongoing investigation into potentially false or misleading claims made by Canada Tax Reviews when it promoted services to Canadians looking to apply for government benefit programs launched in response to the COVID-19 pandemic, including the Canada Emergency Response Benefit and the Canada Recovery Benefit

Office of the Privacy Commissioner

In 2021–2022, the OPC closed 2 complaints it had received in the previous year due to a lack of jurisdiction.

It also received 2 new potential CASL-related complaints. It closed 1 of these due to a lack of jurisdiction, but concluded the other (which concerned unsolicited commercial emails) using the early resolution investigative process.

Thanks to CASL's amendments to PIPEDA in 2011, the OPC was able to collaborate and share information easily with other data protection authorities on compliance and enforcement matters. It also shared information and cooperated with various international counterparts.

In Canada, the OPC collaborated on investigations with privacy enforcement counterparts in Alberta, British Columbia, Québec and Ontario:

- The office continued to work with these provinces on a joint investigation of the Tim Hortons' mobile app. The investigation focused on the app's collection, use and disclosure of users' geolocation data. (A report will be issued in fiscal year 2022–2023.)

- The office investigated a complaint against a company that administered COVID-19 tests at the Montréal–Trudeau International Airport. The federal government required travellers arriving from other countries to submit to such testing. However, some travellers later received emails promoting the company's services without having consented to do so. After the company received complaints from several travellers, it proactively stopped sending the emails and removed the travellers' email addresses from its database. The matter was settled during the investigation. The OPC and the Commission d'accès à l'information du Québec shared information related to the complaint to help resolve it.

The OPC also worked with its provincial counterparts to ensure organizations addressed the recommendations that had emerged after previous investigations:

- Along with the CAI, the office followed up with the Fédération des caisses Desjardins du Québec, which was taking steps to improve its information security, privacy safeguards and data destruction practices after a major privacy breach.
- In December 2021, provincial privacy authorities in Alberta, British Columbia and Québec issued legally binding provincial orders against Clearview AI that required the company to comply with recommendations regarding its facial recognition technology. These orders emerged from an earlier joint investigation that the OPC was involved in. (The OPC does not have equivalent order-making powers under PIPEDA.)

Summary

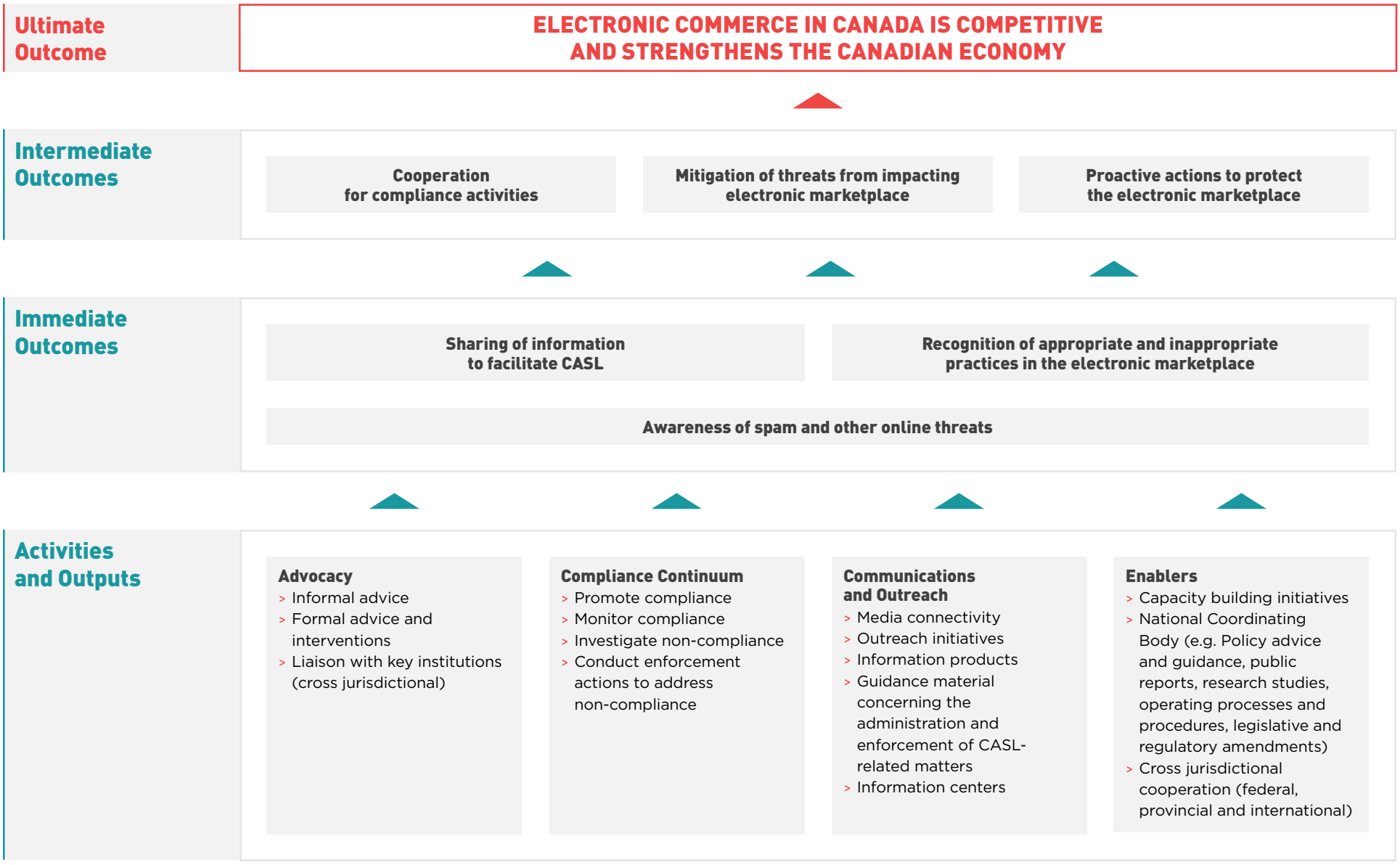
The 2021 calendar year was unprecedented in terms of the volume of cyber attacks. Many of the cybersecurity trends that emerged in 2020 persisted, with malware and ransomware wreaking significant havoc on individuals and organizations around the world.

The ubiquity of electronic threats underscores the importance and relevance of the CASL initiative in continuing to help protect Canadians from spam and other electronic threats that can lead to harassment, identity theft and fraud.

In fiscal year 2021–2022, CASL partners continued to ensure the effectiveness of the CASL regime by taking numerous individual and collaborative steps to promote awareness of and compliance with CASL. They also continued to forge partnerships with organizations across the globe to better fulfill their respective mandates.

This performance report highlights the results of the CASL partners' efforts in 2021–2022. In the coming year, the partners will continue to build a stronger and even more efficient CASL initiative to continue to protect Canadian consumers and businesses from electronic threats.

Annex A: CASL Logic Model



Description

TThe 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 1 ultimate outcome: electronic commerce in Canada is competitive and strengthens the Canadian economy.