

## CASL Enforcement Decision – Interpretive Guidance for Compliance and Penalties

On October 19, 2017, the Canadian Radio-television and Telecommunications Commission issued *Compliance and Enforcement Decision CRTC 2017-368* in a contested enforcement proceeding, imposing a \$200,000 penalty on Compu.Finder for violating Canada's Anti-Spam Legislation (commonly known as "CASL") by sending 317 commercial emails without the recipients' consent and in some instances without a compliant unsubscribe mechanism. The decision provides important guidance for the interpretation of CASL and the CRTC's approach to penalties for CASL violations.

### CASL

CASL creates a comprehensive regime of offences, enforcement mechanisms and potentially severe penalties designed to prohibit unsolicited or misleading commercial electronic messages ("CEMs"), the unauthorized commercial installation and use of computer programs on another person's computer system and other forms of online fraud.

For most organizations, the key parts of CASL are the rules for CEMs. Subject to limited exceptions, CASL creates an opt-in regime that prohibits the sending of a CEM unless the recipient has given consent (express or implied in limited circumstances) to receive the CEM and the CEM complies with prescribed formalities (e.g. sender information and an effective and promptly implemented unsubscribe mechanism) and is not misleading. An organization that sends a CEM has the onus of proving that the recipient consented to receive the CEM.

CASL violations can result in potentially severe administrative monetary penalties ("AMPs") – up to \$10 million per violation for an organization and \$1 million per violation for an individual – in regulatory enforcement proceedings. CASL includes a private right of action, which is not in force. For more information, see BLG bulletin *CASL – Government Suspends Private Right of Action*.

The Canadian Radio-television and Telecommunications Commission (the "CRTC") is responsible for enforcing CASL's CEM rules, and has various enforcement tools for that purpose (e.g. preservation demands, production notices and warrants). Since CASL came into force in 2014, the CRTC has taken enforcement action against organizations and individuals who have violated CASL's CEM rules, and has issued enforcement decisions and accepted voluntary undertakings (settlements). For more information, see BLG bulletins *CASL – Year in Review 2016* and *CASL – Year in Review 2015*.

### The Compu.Finder Investigation and CRTC Decisions

Between July and September 2014, Compu.Finder conducted three unsolicited email campaigns advertising its educational and training services. Complaints to the [Spam Reporting Centre](#) led to an investigation that resulted in the March 2015 issuance of a notice of violation imposing a \$1.1 million AMP on Compu.Finder. For more information, see BLG bulletin *CRTC Issues \$1.1 Million Penalty for CASL Violation*.

Compu.Finder applied to the CRTC for review of the notice of violation. Compu.Finder argued that its emails were exempted from CASL or were sent based on implied consent, and complied with CASL's other requirements. Compu.Finder challenged the fairness of the investigation, and asserted potential bias and inadequate disclosure of information by the investigator. Compu.Finder also challenged the constitutionality of CASL.

In *Compliance and Enforcement Decision CRTC 2017-367*, the CRTC held that CASL was within the legislative competence of Canada's federal Parliament, and did not violate the *Canadian Charter of Rights and Freedoms*. The CRTC reasoned that CASL imposes a demonstrably justified infringement on constitutionally protected freedom of commercial expression, and does not infringe other rights protected by the Charter.

In *Compliance and Enforcement Decision CRTC 2017-368*, the CRTC held that Compu.Finder violated CASL's CEM rules by sending 317 commercial electronic messages without consent and without a compliant unsubscribe mechanism. The CRTC held that the \$1.1 million AMP set out in the notice of violation was not justified by the relevant circumstances, and instead imposed a \$200,000 AMP.

## Interpretive Guidance

The CRTC's decision provides important guidance for the interpretation and application of CASL's CEM rules and the assessment of AMPs. Following is a summary of the guidance.

### 1. Business-to-Business Exemption

The business-to-business exemption set out in section 3(a)(ii) of the *Governor in Council Electronic Commerce Protection Regulations* provides that CASL's CEM rules do not apply to a CEM that is sent by an employee or other representative of an organization to an employee or other representative of another organization if: (a) the organizations have a relationship; and (b) the CEM concerns the activities of the CEM-receiving organization. The CRTC's decision explains:

- The required relationship between organizations will not be established by the mere fact that the CEM-receiving organization has paid for services provided to one or two of its employees by the CEM-sending organization, or the fact that there was some correspondence between the organizations.
- The required relevance of CEMs to the activities of the CEM-receiving organization is not established by the mere fact that the organization's employees previously purchased services advertised by the CEMs, because those employees might have purchased those services for personal reasons unconnected with the activities of their employer organization.
- The required relevance of CEMs to the activities of the CEM-receiving organization is also not established by the mere fact that CEMs were previously sent to the organization.

### 2. Implied Consent to Send CEMs

The conspicuous publication rule set out in CASL section 10(9)(b) provides that consent to receive a CEM is implied if: (a) the person to whom the message is sent has conspicuously published, or has caused to be conspicuously published, the electronic address to which the CEM is sent; (b) the publication is not accompanied by a statement that the person does not wish to receive unsolicited CEMs at the electronic address; and (c) the message is relevant to the person's business, role, functions or duties in a business or official capacity. The CRTC's decision explains:

- The rule requires more than the simple public availability of an electronic address, and applies only in limited circumstances in which consent can be reasonably inferred on a case-by-case basis. An organization that relies on the conspicuous publication rule to send CEMs must establish that all of the requirements of the rule are satisfied.

- The rule will not apply to a person's electronic address that is published by a third party on its own initiative (i.e. without the person's consent).
- The rule will not apply to electronic addresses published in a website directory if the website terms of use prohibit the sending of unsolicited emails to published addresses.
- A CEM-sending organization must provide supporting explanations or evidence, not assumptions or speculation, to establish that a CEM is relevant to the recipient's business role, functions or duties.

### 3. Unsubscribe Mechanism

CASL requires that a CEM "clearly and prominently" set out an unsubscribe mechanism that is "able to be readily performed". The CRTC's decision explains:

- A CEM that contains two unsubscribe links – one link that functions properly and a second link that does not function – does not satisfy CASL's requirements for an unsubscribe mechanism that is "clearly and prominently" set out and is "able to be readily performed", because the two links may cause confusion and frustration by recipients who wish to unsubscribe from CEMs.

### 4. Due Diligence Defence

The due diligence defence set out in CASL section 33 provides that an organization must not be found to be liable for a CASL violation if it exercised due diligence to prevent the commission of the violation. The CRTC's decision explains:

- The onus is on an organization to demonstrate that it exercised due diligence, which generally requires that the organization took all reasonable steps to avoid the CASL violation.
- Activities after a CASL violation occurs will not establish a due diligence defence to liability for the violation.
- To establish a due diligence defence to a CASL violation, an organization must have routine practices, written policies, auditing mechanisms and proactive compliance monitoring during the actual period of the violation, which would have served to prevent or mitigate the violation.

CRTC's *Compliance and Enforcement Information Bulletin 2014-326* provides guidance for a CASL compliance program.

## 5. Amount of AMP

CASL section 20(3) sets out the factors that must be taken into consideration when determining the amount of an AMP, including general deterrence, the nature and scope of the CASL violation, ability to pay, cooperation with investigation, self-correction and proportionality. The CRTC's decision explains:

- **Purpose of Penalty:** The purpose of an AMP is to promote compliance with CASL. General deterrence can be considered when determining the amount of an AMP, but the objective of general deterrence cannot override the requirement that an AMP not lead to the imposition of true penal consequences. The amount of an AMP must be representative of the CASL violations committed and provide enough of an impact on an organization to promote changes in behaviour, both generally and specifically. A significant AMP may be necessary to deter non-compliance or ensure that the risk of an AMP is not viewed as simply another cost of doing business, but the amount of an AMP should not be out of proportion to the amount required to achieve CASL's regulatory purposes. An AMP should not preclude an organization from continuing to operate on a commercial basis.
- **Nature/Scope of Violation:** The relevant nature and scope of a CASL violation includes the disruption, nuisance and frustration caused by unsolicited CEMs.
- **Ability to Pay:** The annual revenues of an organization, particularly a small organization that is privately and closely held, are generally a more reliable indicator of ability to pay than are the organization's annual profits.
- **Cooperation:** An organization's cooperation with an investigation is an important consideration that will be a relevant factor in determining the amount of an AMP in most cases, because cooperation promotes more effective administration of CASL and compliance with other CASL requirements (e.g. preservation demands and notices to produce).
- **Self-Correction:** An organization's self-correction activities will be a relevant factor in determining the amount of an AMP in most cases, because the necessity for, or the amount of, an AMP may

be diminished if an organization has already undertaken efforts to comply with CASL and to correct non-compliance as swiftly as possible. Conversely, an organization's demonstrated reluctance or unwillingness to correct CASL violations may increase the necessity for an AMP or the amount that will be considered appropriate.

- **Proportionality:** The proportionality of an AMP is a function of how the relevant factors set out in CASL apply to the circumstances of an individual case. If an AMP reasonably reflects the relevant factors, then the AMP will be proportionate and serve its regulatory purpose.

## Comment

CASL is currently under statutory review by the federal government, and might be amended as a result. In the meantime, CASL remains subject to regulatory enforcement, which can involve time-consuming and costly investigations and proceedings and result in potentially significant AMPs.

There are a number of important steps that an organization should take to enhance its CASL compliance and mitigate the risks of regulatory enforcement, including: (1) review/update its CASL compliance program; (2) verify its due diligence documentation; and (3) review/update its CASL complaint/litigation response plan. For more information, see BLG bulletins *Canada's Anti-Spam Legislation – Regulatory Guidance* and *CASL Compliance Programs – Preparing For Litigation*.

Organizations should be mindful that Canadian privacy laws regulate the collection, use and disclosure of certain kinds of personal information used to send CEMs. Accordingly, organizations should ensure that their marketing activities comply with both CASL and applicable privacy laws. For more information see BLG bulletin *Canadian Privacy Commissioner Issues Guidance for Privacy Law and CASL Compliance*. ■

## Author

**Bradley J. Freedman**

T 604.640.4129

bfreedman@blg.com

BLG's national CASL Group includes lawyers, located in BLG's offices across Canada, with expertise in CASL, privacy law, cyber risk management and class action litigation. We provide both proactive CASL compliance advice and legal advice to help respond to a CASL contravention, including acting as legal counsel in regulatory proceedings and defending class litigation. Additional information about BLG's national CASL Group and our services is available at [blg.com/CASL](http://blg.com/CASL).

**BORDEN LADNER GERVAIS LLP**  
LAWYERS | PATENT & TRADEMARK AGENTS

Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.

*This document provides general information only, and does not constitute legal or other professional advice. Readers are encouraged to obtain legal advice from a competent professional regarding their particular circumstances.*  
Copyright © 2017 Borden Ladner Gervais LLP.

**BLG Vancouver**

1200 Waterfront Centre, 200 Burrard St  
Vancouver, BC, Canada V7X 1T2

T 604.687.5744 | F 604.687.1415

[blg.com](http://blg.com)