

CASL enforcement – \$100,000 penalty for sending messages and installing software without consent

On September 30, 2020, the Canadian Radio-television and Telecommunications Commission announced that Canadian student note-sharing platform OneClass paid \$100,000 as part of a settlement of alleged violations of Canada's Anti-Spam Legislation (commonly known as "CASL"). The alleged CASL violations related to sending commercial electronic messages without consent and installing computer software without consent.

CASL

CASL creates a comprehensive regime of offences, enforcement mechanisms and potentially severe penalties designed to prohibit the sending of unsolicited 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. Following are some key aspects of CASL:

- CASL creates an opt-in regime that prohibits, subject to limited exceptions, 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., information about the sender and an effective and promptly implemented unsubscribe mechanism).
- CASL prohibits, subject to limited exceptions, the installation and use of a computer program on another person's computer system, in the course of a commercial activity, without the express consent of the owner or authorized user of the computer system.

- CASL imposes liability on organizations and individuals (including corporate directors and officers) for both direct and indirect/vicarious CASL violations. CASL provides a due diligence defence.
- CASL violations can result in regulatory penalties of up to \$10 million per violation for an organization and \$1 million per violation for an individual. CASL includes a private right of action that is not in force.

The Canadian Radio-television and Telecommunications Commission ("CRTC") is responsible for enforcing CASL's rules regarding CEMs and computer programs. Since CASL came into force in 2014, CRTC has taken enforcement action against organizations and individuals who have violated CASL, and has issued enforcement decisions and accepted voluntary undertakings (settlements). See BLG bulletins [CASL – Year in Review 2019](#), [CASL – Year in Review 2018](#), [CASL – Year in Review 2017](#), [CASL – Year in Review 2016](#) and [CASL – Year in Review 2015](#).

Investigation and settlement with OneClass

The CRTC's [announcement](#) and published [undertaking](#) (settlement agreement) with OneClass explain that the CRTC's investigation alleged that:

1. between October 2016 and March 2020, OneClass sent, or caused to be sent, CEMs to promote its student note-sharing platform without obtaining the required consent from CEM recipients; and
2. between October and November 2016, OneClass installed on post-secondary students' computer systems, without their valid consent, a chrome browser extension that collected personal information (including usernames and passwords) stored on the computer systems contrary to the reasonable expectations of the owners or users of those computer systems.

The settlement agreement requires OneClass to pay a \$100,000 administrative penalty and comply with the following obligations:

- Comply with CASL and ensure that any third party authorized to send CEMs or install computer programs on OneClass's behalf complies with CASL.
- Develop and implement a CASL compliance program for the sending of CEMs, including corporate compliance policies and procedures, employee training and education, and monitoring, auditing and reporting mechanisms.

- Monitor and review internal policies and procedures to determine whether they provide incentives for employees to violate CASL, and eliminate identified incentives.
- Register and track CASL complaints and the resolution of those complaints.
- Implement effective corrective measures for CASL compliance failures, and maintain regular communications with the CRTC regarding CASL compliance.

The CRTC's announcement of the OneClass settlement references updated [guidance](#) regarding CASL's rules for the installation of computer programs. For more information, see BLG bulletin [CASL – Regulatory guidance for computer program installation rules](#).

Comment

The CRTC's enforcement action against OneClass illustrates the importance of an effective CASL compliance program as a risk management strategy to reduce the likelihood of CASL contraventions and help establish a due diligence defence and ameliorate potential sanctions if a CASL contravention occurs. For more information, see BLG bulletin [CASL Compliance Programs – Preparing for Litigation](#). ■

Author

Bradley J. Freedman

T 604.640.4129

bfreedman@blg.com

BLG's national Compliance with Privacy and Data Protection 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. Additional information about BLG's national Compliance with Privacy and Data Protection group and our services is [available here](#).

blg.com | Canada's Law Firm

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.

© 2020 Borden Ladner Gervais LLP. BD9895-10-20

BLG
Borden Ladner Gervais