

Canada's Anti-Spam Legislation (CASL)

What you need to know to protect yourself—As direct marketing specialists, we at Highland Marketing have been thoroughly combing through the details of Canada's Anti-Spam Legislation (CASL), and we want to share our knowledge and insights with you.

Never heard of CASL? No problem! We've put together this brief guide as an introduction, to give you a synopsis of the legislation, and to provide an overview as to what activities to avoid, what activities to pursue, and what implications these activities might have on your business.



Disclaimer: While we have made every effort to represent the information contained herein in accordance with our understanding of Canada's Anti-Spam Legislation, Highland Marketing makes no guarantee as to the completeness and/or accuracy of this document and shall not be held responsible for any damages resulting from its use. This document is provided as a general introduction to CASL. It should not be considered as legal counsel or as a substitute for reading the actual legislation.

Understanding CASL

So what is Canada's Anti-Spam Legislation (CASL)? It is Canada's newest method of combating spam sent in the form of commercial electronic messages (CEMs) to electronic addresses. Examples of these types of messages include: e-mail, Short Message Service (SMS), Multimedia Message Service (MMS), private messages through social media, and even Voice Over Internet Protocol (VoIP) communications. Basically, if you're sending a message that solicits business, and that will be received by an electronic address, assume that CASL applies.

There are 3 key rules for sending compliant messages:



Be Sure To Have Consent

Consent can be either **Express**, explicitly obtained through opt-in, or **Implied**, implicitly obtained through a business relationship.



Identify All Senders

Messages must **identify** and **provide contact information** for the party sending the message *and* the party on behalf of whom it is being sent.



Include an Opt-Out Mechanism

Messages must include a **simple, quick, easy and free method of opting-out**, which must be honoured within 10 days of the request.

Following these 3 rules will ensure that you're safe to send your commercial electronic messages (CEMs).

Since obtaining consent has quite a few pitfalls associated with it, it is important to explain the types of consent, methods for obtaining consent, and the guidelines surrounding them.

Express consent only expires if the recipient opts-out of your messages. It also comes in 2 flavours, express consent and third party express consent. The details for each are as follows:

Express Consent

The recipient actively chooses to opt-in to receive your messages. This means that the recipient had to toggle into the consent, that the consent was not bundled with any other consent or offers, and that the opt-in was not solicited through an electronic message.

Express consent is much more desirable than implied consent, because it is obtained in a very straightforward manner, that is not open to interpretation.

Third Party Express Consent

You are allowed to seek consent for unknown third parties to send messages to your recipients. However, the same general express consent rules apply, along with some additional requirements.

Each and every third party must provide an opt-out mechanism from third party consent. If an opt-out is received, the third party must notify the original requester, and in turn, the original requester must notify all third parties of the consent withdrawal.

Implied consent is a bit more complex than express consent, and expires at different times, depending on how it was obtained.

Implied Consent

The recipient has a previous business relationship with you. Implied consent expires 6 months following an inquiry or application, and 2 years following your most recent business transaction with the recipient.

It should also be noted that you are no longer allowed to collect or use personal information obtained by harvesting, scraping or hacking. In essence, information that is posted publicly does not come with implied consent.

Transitional Provisions for Implied Consent

If the recipient's implied consent was obtained before July 1, 2014, then it will expire if the recipient doesn't opt-in by July 1, 2017.

CASL "Death Moves"

Failure to comply with CASL can have some *serious consequences*, including fines of up to \$1,000,000 for individuals, and up to \$10,000,000 for businesses. Moreover, you could face criminal charges, or open yourself up to legal liabilities. To help you stay compliant, we've put together this list of "death moves" that you *will want to avoid* when sending commercial electronic messages (CEMs):

- × Harvesting electronic addresses and personal information
- × Requesting consent via CEM
- × Bundling express consent to receive CEMs with other consents or agreements
- × Pre-toggling opt-ins
- × Sending CEMs to recipients you do not have consent from
- × Sending CEMs to recipients whose implied consent has expired or been withdrawn
- × Sending CEMs to recipients who have withdrawn their express consent
- × Sending CEMs without clearly identifying the sender
- × Sending CEMs without clearly identifying the primary consent requester
- × Sending CEMs without accurate contact information of the sender
- × Sending CEMs without accurate contact information of the primary consent requester
- × Sending CEMs without a valid, free, quick and simple opt-out mechanism
- × Not honouring opt-out requests within 10 days
- × Not alerting the primary consent requester of a request to withdraw third party consent
- × Not alerting all third parties of withdrawal of third party consent

More questions? No problem! We would love to chat and help answer any questions you may have about CASL. Call us at 1-800-422-1309.