POSSIBLENOW®

Marketing Compliance Made Simple

CASL OVERVIEW GUIDE

THE CANADIAN ANTI-SPAM LAW

By Eric Tejeda, VP of Marketing

WHAT'S INSIDE

Introduction

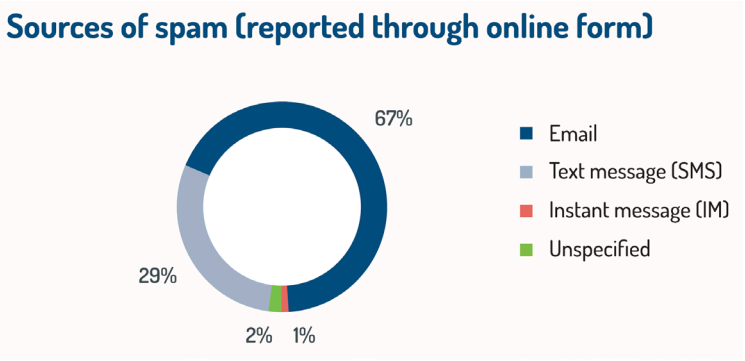
The Canadian Anti-Spam Law (CASL) went into effect back in 2014 but it still pertains to communications sent to Canadian residents and the financial penalties can be severe. It's easy to brush off CASL and give more attention to regulations like GDPR and CCPA, but if your organization is in Canada or sends communications to Canadian residents, you need to be complying with CASL.

CASL was implemented to control and regulate the sending of CEMs (Commercial Electronic Messages) to combat spam and create an opt-in environment. It affects communications sent to email addresses, phone numbers (which includes text or SMS messages), social media accounts, or instant messaging accounts.

A CEM is any message:

- in an electronic format. This includes emails, instant messages, text messages (SMS), and some social media communications (such as tweets);
- sent to an electronic address. This includes email addresses, instant message accounts, phone accounts, and social media accounts;
- containing a message encouraging recipients to take part in some type of commercial activity. This includes the promotion of products or services, people, and companies or organizations.

Fax messages and fax numbers are not considered electronic formats or addresses under CASL.



Source: Canadian Radio-Television and Telecommunications Commission, https://crtc.gc.ca/eng/internet/pub/20240930.htm

CASL Requirements

All CEMs must include certain requirements to be compliant under CASL:

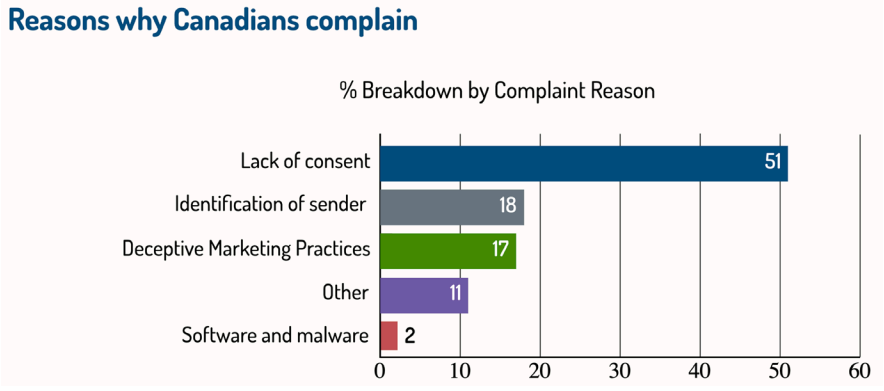
- the name of the sender, or the name of the person/business on whose behalf it is sent
- a mailing address and at least one of the following:
    - a telephone number providing voice messaging
    - an email address
    - or a web address of the sender, or if different, the name of the person or business on whose behalf it is sent
- an easily-accessible method to unsubscribe

For short CEMs, like text (or SMS) messages or tweets, a clear and prominent link to a web page can substitute for this information, as long as it's easily accessible and at no cost to the recipient.

Requests for consent to contact a recipient can be made orally or in writing, but must include the same components listed above to identify the sender of the CEM (or on whose behalf the CEM is being sent) as well as a statement that the recipient can withdraw their consent.

Both implied consent and express consent to send communications affect CASL liability. Implied consent allows organizations to send CEMs for 6 months to inquiries and up to 24 months to current or prior customers. A sender can imply consent if an "existing business relationship" (EBR) exists within the prior two years, or if the intended recipient has either disclosed or published their contact information without any indication that they do not wish to receive unsolicited CEMs.

Express consent is considered valid indefinitely unless or until the contact specifically unsubscribes. These timeframe limitations must be carefully managed to prevent exposing your organization to potential liability.



Source: Canadian Radio-Television and Telecommunications Commission, https://crtc.gc.ca/eng/internet/pub/20240930.htm

Fines and Exclusions

CASL is enforced by the Canadian Radio-Television and Telecommunications Commission (CRTC), and violations can be very costly. Aside from the public relations damage to your organization's brand and reputation, the possibilities for financial penalties can be as high as:

$1 million penalty per violation for individual offenders
$10 million penalty per violation for organizations

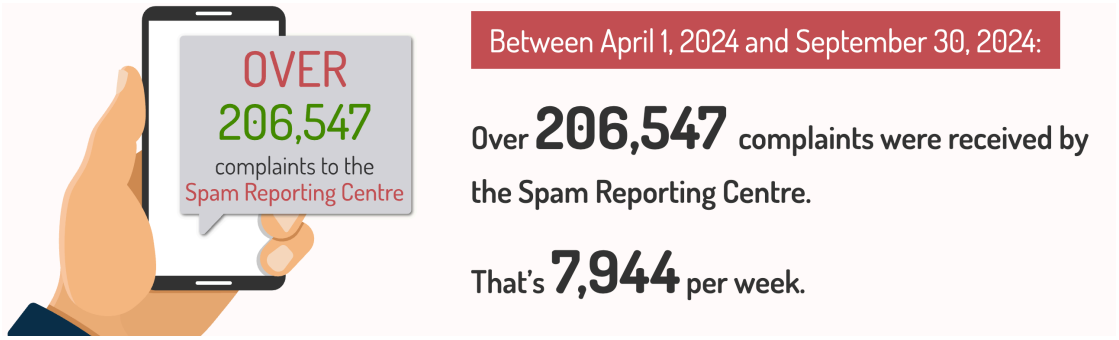
A few exclusions do apply. Some of the exclusions currently listed include:

- CEMs sent in the context of a personal or family relationship
- Inquiries sent directly to a person engaged in a commercial activity about their business – such as a question or complaint

In addition, consent isn't required in several scenarios. For example, CEMs coming from organizations whose purpose is to:

- Provide a quote or estimate
- Respond to an inquiry or complaint
- Facilitate a commercial transaction
- Provide warranty or safety information
- Provide information about an ongoing service or product sale
- Provide information about employment information
- Complete a sale or delivery

So with all those exclusions, what counts as a violation?



Source: Canadian Radio-Television and Telecommunications Commission, https://crtc.gc.ca/eng/internet/pub/20240930.htm

According to CASL, each of these examples would be considered violations:

- Sending of CEMs without consent;
- Sending CEMs lacking the required identifying information or unsubscribe feature;
- Alteration of transmission data in an electronic message which results in the message being delivered to a different destination without express consent;
- Installation of computer programs without the express consent of the owner of the computer system or its agent, such as an authorized employee;
- Use of false or misleading representations online in the promotion of products or services;
- Collection of PI (personal information) through accessing a computer system in violation of federal law (e.g. the Criminal Code of Canada); and
- Collection of electronic addresses by the use of computer programs or the use of such addresses, without permission (address harvesting).

Who needs to pay attention to CASL?

- CMO/marketing executives need to review their digital marketing campaigns for vulnerabilities, especially those run through email and social media. They must also develop a plan to obtain consent for communications.
- Chief legal counsel must review CASL's requirements, changing regulations and commentary from industry associations, and monitor any regulatory guidance and interpretive guidelines released by the government.
- Risk officers need to assess the risks of CASL non-compliance on the business and work with compliance and business teams to mitigate these risks.
- Internal auditors must evaluate CASL compliance once it is in force, independent of the business.

How to Plan for CASL Compliance

Many organizations may not even be aware that CEMs are being sent to electronic addresses where the CEM will be accessed in Canada. Organizations should audit their electronic address databases to determine if CEMs are sent to Canadian addresses.

Although the steps each organization must take will vary, to properly prepare for CASL compliance, you should:

- Determine if you are sending CEMs as defined by the CRTC
- Identify the channels through which you send CEMs. Is it through text, email, social media accounts? All of these?
- Assess if you have implied or express consent to send CEMs or if an exemption applies for each situation
- Develop a plan to obtain any required consents
- Make sure your CEMs contain the content required by CASL – identifying information and unsubscribe capability
- Determine how CASL may affect your policies, processes, customer relationship management (CRM) and other IT systems, and staff training and awareness programs
- Revise those policies, processes, and systems as required
- Keep an audit trail, since CASL contains a "due diligence" defense

TIP!

Organizations can determine whether the message is sent to a Canadian CEM by auditing the following in their databases:

- A Canadian physical address is associated with the electronic address;
- An email ends with the .ca internet country code; and/or
- A telephone number has a Canadian area code.

If any of these

How PossibleNOW Can Help:

PossibleNOW's DNCSolution offers a comprehensive feature set to ensure compliance with all relevant Do Not Contact compliance laws both in the United States and Canada. Our SOC 2 compliant platform supports the high-volume DNC scrubbing and maximum service availability needs of direct marketers.

MyPreferences integrates with DNCSolution to store all consumer consents and preferences, allowing for easy consent capture and revocation of consents, to keep you compliant.

PossibleNOW is the pioneer and leader in customer contact compliance. From federal and state regulations to international laws, our platform DNCSolution consolidates everything a business needs to stay compliant with regulations such as Do Not Call, TCPA, CAN-SPAM, and Reassigned Numbers Database. We back our solutions with a 100% compliance guarantee and keep companies out of the crosshairs of professional litigators.

Our MyPreferences platform centralizes the collection and distribution of customer communication consents and preferences, making compliance and personalization possible across the enterprise.

PossibleNOW's strategic consultants take a holistic approach, leveraging years of experience when creating strategic roadmaps, planning technology deployments, and designing customer interfaces.

Our technology, processes and services enable relevant, trusted, and compliant customer interactions.

PossibleNOW: Marketing Compliance Made Simple.

CONTACT

Contact Us

(800) 585-4888 or (770) 255-1020

email | info@possiblenow.com

visit | www.possiblenow.com