CASL Survey Report

Bridging the Gaps in Understanding and Compliance

PRIVACY AND INFORMATION PROTECTION GROUP

dmac DIRECT MARKETING ASSOCIATION OF CANADA

FASKEN

Table of Contents

CASL Survey Report - Bridging the Gaps in Understandingand Compliance 1

A. Summary 3

B. Respondents 5

C. Findings 7

D. CASL Compliance Implementation and the Due Diligence Defence 9

E. Conclusion and Recommendation 13

APPENDIX - Survey Questions, Answers and Commentary 15

CASL SURVEY REPORT

Bridging the Gaps in Understanding and Compliance

In March 2017, the Direct Marketing Association of Canada (DMAC) and Fasken set out to determine the current state of understanding and compliance with Canada's anti-spam legislation (CASL) across small, medium and large organizations. Anecdotal evidence at the time suggested that organizations were operating under a false sense of security about their CASL comprehension and compliance, despite the legislation being in force for almost three years. To gain a deeper understanding of these matters, a survey was composed and circulated to mailing lists for DMAC, Blazon.Online and Fasken.

The results are in. With well over 200 respondents, our CASL survey provides a revealing spot check on the extent to which organizations understand CASL, and what is required to implement effective compliance strategies and due diligence defence measures. Survey results were provided by those who would be familiar with the legislation – over 80% of respondents were either extremely involved or very involved in the design and implementation of their organization's CASL strategy.

Special thanks to all those who participated.

A. Summary

As our survey results show, even after almost 3 years of CASL being in force, there is still a notable lack of understanding about key elements of the law, and an even larger gap when it comes to understanding how it should be implemented to ensure full compliance. Organizations should already be compliant.

Since 2014, the Canadian Radio-Television and Telecommunications Commission (CRTC) has conducted investigations, entered into undertakings, issued notices of violation and imposed administrative monetary penalties (AMPs) on a number of organizations for failure to comply with one or more elements of CASL. With the so-called "private right of action" set to come into force on July 1, 2017, organizations need to urgently revisit CASL to ensure that their house is in order. As supported by our survey results, many who think they are compliant still have a way to go. While progress has been made, significant work must still be done across all sectors and all sizes of organization.

DEFINITIONS

CASL	Canada's Anti-Spam Legislation
CEMs	Commercial Electronic Messages
AMPs	Administrative Monetary Penalties
B2B	Business – To – Business
B2C	Business – To – Consumer
DMAC	Direct Marketing Association of Canada
CRTC	Canadian Radio-Television and Telecommunications Commission

Organizations should already be compliant.

B. Respondents

Industries represented among respondents

- agriculture
- automotive
- chemical/pharmaceutical
- construction
- computer/software/information technology
- consulting
- education
- engineering
- health care
- hospitality
- legal
- manufacturing
- marketing
- music/film/entertainment
- publishing
- retail
- telecommunications
- transportation/logistics

The industry group with the largest percentage of respondents was the financial services industry (21% of respondents). For-profit organizations made up the majority of respondents (approximately 77%) across all size categories.

Organizations of all sizes based on number of employees (0-9, 10-99, 100-499, 500-999, 1000+) were well represented, particularly medium-sized organizations (10-499). Small companies (0-9) had the fewest respondents. Companies with more than 1000 employees represented 21% of our findings.

The primary nature of respondents' marketing and business development activities was roughly equal between B2B and B2C. E-marketing was a significant part of the marketing strategy for 60% of respondents. However, it is important to note that an organization that conducts any e-marketing, whether or not it is a significant part of their marketing strategy, should be concerned about CASL compliance. CASL applies regardless of the volume of commercial electronic messages (CEMs) that an organization sends.

CASL applies regardless of the volume of commercial electronic messages (CEMs) that an organization sends.

C. Findings

The results of the survey are detailed in the appendix to this report, together with correct answers and associated commentary. Of significant concern is that many fundamental aspects of CASL are still not well understood – such as the types of messages governed by CASL, whether the sending of certain CEMs requires consent or an exemption, and how express consent can be obtained. The results also indicate a need to better understand the content requirements for CEMs.

Some of the confusion may result from a mistaken belief that CASL's requirements mimic those found in corresponding US legislation. On the contrary, CASL establishes a higher standard than the US's *CAN-SPAM Act*. The US legislation may have been the cause for the apparent confusion about whether CASL applies to CEMs sent into Canada from the US (or from any other jurisdiction).

When it comes to the consequences of non-compliance, many respondents did not appreciate the extent of potential AMPs, or when AMPs could be imposed by the CRTC. Many were also unaware that directors and officers could be held personally liable for breaches of CASL. It would also appear that the exposure to statutory damages is not well understood.

Of equal concern is the apparent lack of appropriate policies and procedures, including record-keeping programs, within many organizations to support and evidence compliance with CASL. Respondents stated that their organizations lack compliance programs involving written policies, employee training and regular compliance audits. Few have confidence that their organization could establish how consent was obtained, or that CEMs sent by their organization contained the required content and a properly functioning unsubscribe mechanism.

Many fundamental aspects of CASL are still not well understood.

More than half of respondents could not confirm that their organization had written contracts with their e-marketing service providers – exposing them to additional risk.

The results of the survey are somewhat alarming, given that organizations are currently exposed to enforcement action by the CRTC (and potentially the Privacy Commissioner of Canada and the Competition Bureau). In light of the survey results, organizations should be taking this opportunity to avoid greater liability exposure by addressing shortcomings prior to the private right of action coming into force.

Many organizations appear to lack appropriate policies and procedures, including record-keeping, to support and evidence compliance with CASL.

D. CASL Compliance Implementation and the Due Diligence Defence

As referenced in Section C, above, the survey results indicate that there is still a notable gap in understanding what an organization should do to be prepared to respond to an allegation of non-compliance with CASL. Under CASL, a person who alleges that they have consent to do an act that would otherwise be prohibited by the anti-spam provisions of CASL has the onus of proving it. This raises an obligation that is not clearly spelled out in CASL – the obligation to maintain evidence of compliance. Without sufficient evidence, compliance essentially does not exist. Organizations, therefore, should be as concerned about record-keeping as they are with meeting the requirements of CASL.

CASL also provides that a person will not be liable for a violation if they establish that they exercised due diligence to prevent the commission of the violation. Accordingly, organizations should be positioning themselves to take advantage of this due diligence defense. The survey results support the conclusion that many organizations of all sizes are unfamiliar with this defence, or how to arrange their operations so that they can invoke it effectively.

Although CASL does not describe the specific circumstances that would qualify for the due diligence defence, the CRTC has issued guidance in a variety of forms. The notices of violation issued by the CRTC and the undertakings entered into by various organizations in favour of the CRTC as it relates to CASL, as well as CRTC Compliance and Enforcement Information Bulletin 2014-326: "Guidelines to help businesses develop corporate compliance programs", provide insight into the types of activities that organizations should consider implementing to support compliance with CASL.

This guidance can be distilled into the best practices listed on the next pages.

Without sufficient evidence, compliance essentially does not exist.

1. Establish an organization-wide CASL compliance program

Establishing and documenting an organization-wide CASL compliance program helps to ensure that all departments of an organization handle e-marketing matters in a similar manner and that consistent checks and balances are in place to facilitate ongoing compliance.

To date, CRTC undertakings generally require organizations to adopt (or refresh) a written CASL compliance program. This program should include monitoring, auditing and reporting mechanisms, registration and tracking of complaints and their resolution, measures to resolve compliance failures, and training and education for personnel. The program should also address procedures for dealing with third parties and recordkeeping, especially with respect to consent.

In a number of recent cases, the CRTC considered the existence of a compliance program as a mitigating factor in applying AMPs. Furthermore, an existing compliance program could be used to support a due diligence defence.

The CRTC recognizes that compliance programs will vary depending on the size and risk exposure of the organization.

2. Involve senior management

Senior management should play an active, visible, and vocal role in fostering a culture of compliance, particularly in large organizations, by supporting and enforcing the compliance program. Furthermore, since directors and officers may be held personally liable for violations of CASL, ensuring the involvement of senior management aids in avoiding that personal liability.

3. Appoint a chief compliance officer (CCO)

A CCO can undertake a number of responsibilities to ensure CASL compliance within an organization. The CCO can deal with complaints about the organization's conduct, undertake risk assessments to analyze high-risk business activities, and promptly respond to any communication from the CRTC. The fact that an organization invests in a CCO will be taken into consideration if any complaints are ursued by the CRTC.

Organizations should be positioning themselves to take advantage of the due diligence defence.

4. Formalize a written compliance policy

Having an easily accessible, written compliance policy which establishes internal procedures and provides the name and contact information of the CCO, will ensure that any discrete issues can be dealt with swiftly. This will also allow employees to educate themselves and others. The policy should address the issues discussed below.

5. Education and employee buy-in

Continued compliance with CASL requires the ongoing education of employees and assessment of internal business processes. This can be achieved through training, to educate employees about prohibited conduct and possible pitfalls. Employees can be required to execute a formal document that confirms their understanding of the policy and commitment to compliance. This may be used in establishing a due diligence defence. Furthermore, this establishes a process for employee feedback to improve compliance and practical application of the compliance policy.

6. Record-keeping

Organizations should have a detailed record-keeping system that documents all aspects of compliance, including express and implied consents, unsubscribe requests and fulfillment, customer complaints, compliance issues, the monitoring and auditing of the compliance program, and any corrective actions taken.

7. Complaints and correction

Organizations should provide customers with channels to make complaints. This will establish credibility and allow the organization to respond to complaints expeditiously. The complaints system is not to be confused with the process of withdrawing consent (e.g., responding to unsubscribe requests). Providing for, and giving effect to, a mechanism for withdrawing consent should be clear to recipients and is mandated as a stand-alone process.

In addition, organizations should be able to self-correct. A disciplinary code is a good way to ensure employees self-correct and will establish internal credibility for the compliance program. The CRTC will take both complaints processes and self-correction into consideration when determining AMPs.

More than half of respondents could not confirm that their organizations had written contracts with their e-marketing service providers.

8. Service providers

Under CASL, organizations can be held liable for breaches by their service providers. Therefore, organizations that rely on service providers for any aspect of their e-marketing function should conduct appropriate due diligence on the service provider's operations and processes. In addition, outsourcing any aspect of the e-marketing function should be done pursuant to a written contract that includes appropriate clauses to address each party's responsibilities and liability.

9. Review all communications

All e-marketing campaigns should be reviewed by senior management or a CCO. For example, if a CCO reviews CEMs sent out by email but not those distributed through text message, compliance issues may be missed.

10. Protect servers

If a third party hacks an organization's computer system and uses it to send CEMs in violation of CASL, the organization could nonetheless be held responsible. Even if the organization is not ultimately held responsible, cooperating with a CRTC investigation will result in costly business disruptions. Care should therefore be taken to ensure that the organization's computer systems are secure and that any emails emanating from an organization are initiated by an authorized representative.

11. Auditing and monitoring

Organizations should establish annual audits to assess compliance and reassess business procedures. Results of audits should be documented, analyzed and shared with the COO and other senior management, and used to update the organization's compliance program, as appropriate. Auditing should also extend to all service providers involved in CASL-related activities.

12. Seek help from the experts

Given the complexity and uncertainty that can be associated with many CASL related activities, and the high stakes associated with CASL violations, including how they can overlap with privacy laws in Canada, organizations need to work carefully with their internal and external legal counsel, marketing specialists, compliance and risk managers, insurance brokers and other experts to understand and manage CASL risks.

E. Conclusion and Recommendation

Organizations have a lot of work to do. Not satisfying CASL's requirements, and not having an appropriate compliance program in place, could end up being extremely costly. The CRTC's complaint-based system is always at work and their ability to fine up to $10 million per violation presents considerable risk. With the looming "private right of action" due to take effect on July 1, 2017, the public and the plaintiffs' class action litigation bar will join the CRTC as another source of CASL enforcement. While the CRTC's reach may be limited based on current resources, the public's reach, particularly through class action law suits, will not be.

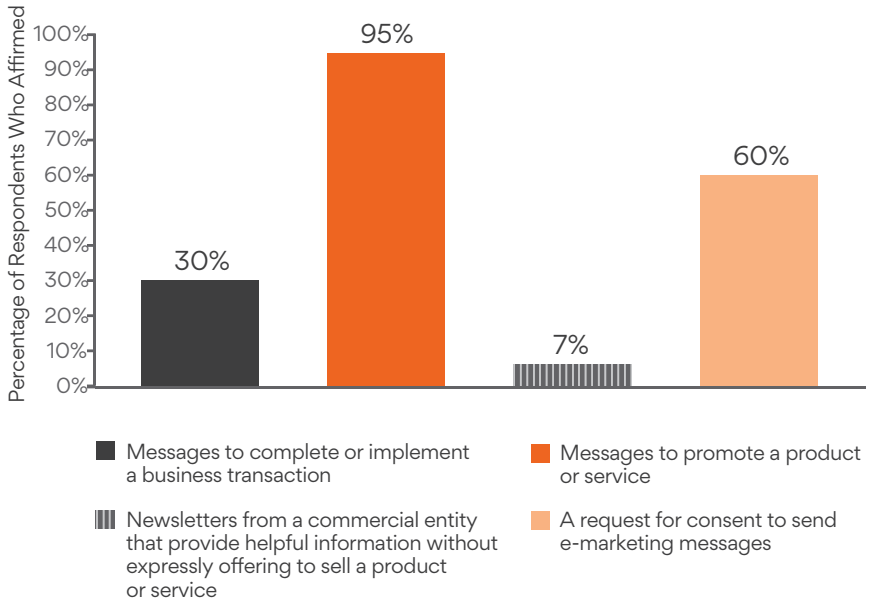
Organizations still have more work to do.

APPENDIX

Survey Questions, Answers and Commentary

What Do You Know About CASL?

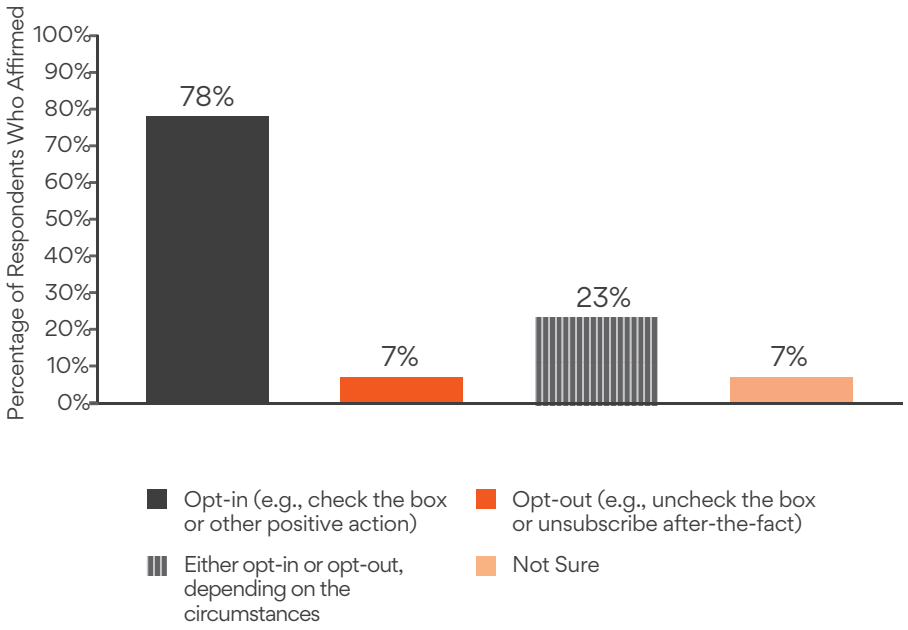
1. **Which of the following types of e-marketing messages would require consent (express or implied) under CASL (check all that apply):**



A message to complete or implement a business transaction does not require consent under CASL. However, the other types of messages referenced in this question would require consent (whether express or implied) or an exemption. Of note, a newsletter from a commercial entity that provides helpful information would seem to inherently promote that organization and, as such, would either be a commercial electronic message (requiring consent or an exemption) or ought to be treated as such (out of caution).

40% of respondents did not appreciate that consent is generally required to send an electronic message requesting consent to send e-marketing messages.

2. **If express consent is required under CASL, that consent can be obtained by (check all that apply):**

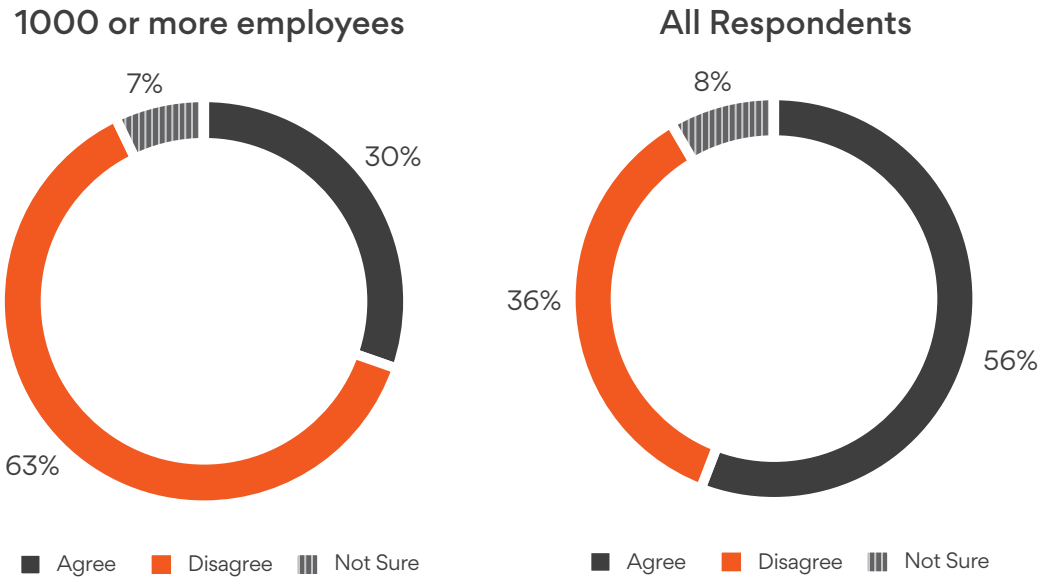


Express consent is one basis on which to send e-marketing messages under CASL. Express consent can only be obtained by an opt-in mechanism, such as checking an unchecked consent box or another positive action by the intended recipient in order to manifest consent.

The advantage in having express consent is that the consent lasts until the recipient unsubscribes – unlike implied consent, which generally expires after a prescribed period of time (unless the recipient has unsubscribed before then).

At least 23% of respondents did not appreciate that "express consent" can only be obtained using an opt-in mechanism.

3. **If consent is obtained, as long as the e-marketing message includes a properly functioning unsubscribe mechanism, that message will be fully compliant with CASL:**



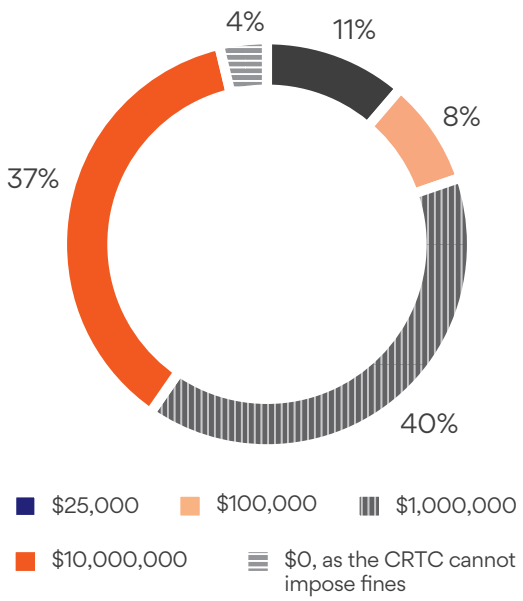
Consent and an unsubscribe mechanism are required but not sufficient. To comply with CASL, the message also needs to include the prescribed identification and contact information for the sending organization (and any organization on whose behalf the message is sent).

In addition, the sending organization needs to be able to demonstrate both that it had sufficient consent to send the message, and that the message contained the required content and unsubscribe mechanism.

Small to medium-sized organizations are more likely to misunderstand this aspect of CASL, and see consent and an unsubscribe mechanism as sufficient to comply with CASL – missing the prescribed message content and the record-keeping requirements.

64% of respondents did not appreciate that a CASL-compliant message requires more than just consent and a working unsubscribe mechanism.

4. **For each violation of CASL, the CRTC can impose an AMP against an organization of up to:**



$10,000,000 is the maximum AMP for organizations. The maximum AMP for individuals is $1,000,000.

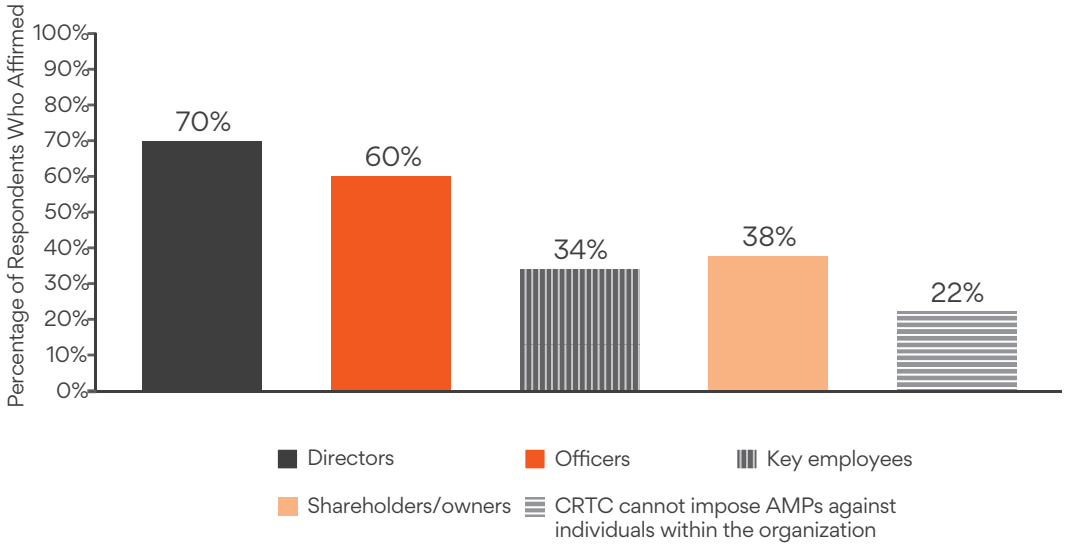
When determining the amount of the AMP, the CRTC will take into consideration a number of factors, such as the nature and scope of the violation, previous contraventions of CASL or related legislative requirements, whether any financial benefit was obtained from the violation, and the person's ability to pay.

To date, AMPs levied by the CRTC have been as high as $1,100,000.

Small to medium-sized organizations are more likely to underestimate their exposure, misperceiving the maximum penalty for organizations at $1,000,000 instead of $10,000,000.

63% of respondents did not know that the CRTC can impose an AMP of up to $10,000,000 for each violation of CASL.

5. **The CRTC can impose AMPs against the following individuals for CASL violations by an organization (check all that apply):**



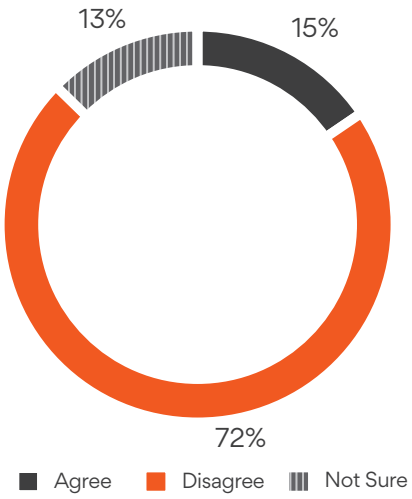
The CRTC can impose AMPs against directors and officers of an organization, as well as against the agents or mandataries of an organization. This liability will arise if that person directed, authorized, assented to, acquiesced in or participated in the commission of the violation.

In addition, an organization can be liable for the actions of its employees, agents and mandatories. CASL provides that a person is liable for a violation that is committed by their employee acting within the scope of their employment or their agent or mandatary acting within the scope of their authority.

This liability is subject to a due diligence defence: a person will not be found to be liable for a violation of CASL if they establish that they exercised due diligence to prevent the commission of the violation.

30% of respondents did not appreciate that directors can be personally liable for CASL violations by their organization, and 40% did not appreciate that officers can be personally liable.

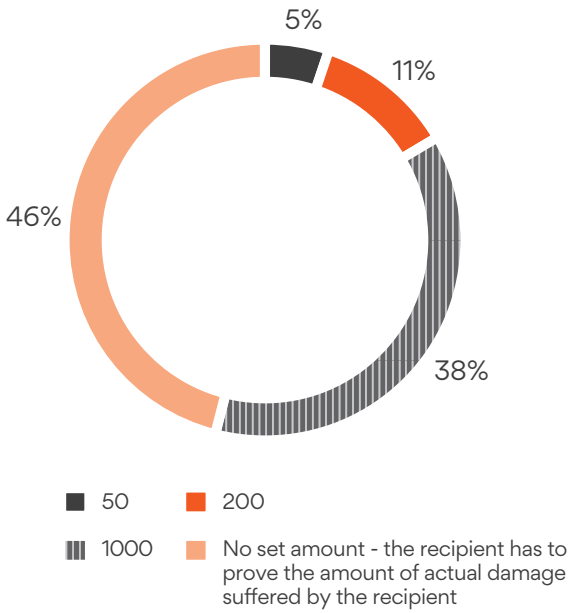
6. **The CRTC can only impose AMPs on an organization if the organization is a repeat offender or has knowingly violated CASL:**



28% of respondents incorrectly believe (or are not sure) that the CRTC can only impose AMPs on repeat offenders or organizations that knowingly violate CASL. All AMPs and undertakings to date have been for first offenders.

As discussed earlier, CASL includes various factors that the CRTC must consider when determining an AMP for a violation of CASL. One of these factors is whether the organization has previously breached CASL or any related legislation. The presence or absence of this factor may go to the amount of the AMP, but is not determinative; the CRTC can impose an AMP for a first-time violation of CASL.

7. **Under the "private right of action", if an organization sends an e-marketing message to a recipient in contravention of CASL, that recipient will be entitled to recover the following amount for each contravention (up to a maximum of $1,000,000 for each day on which the contravention occurred):**



The "private right of action" involves statutory damages of up to $200 for each contravention, without any need for the recipient to prove that the recipient actually suffered any damages. These statutory damages are in addition to any actual damages that the recipient can prove.

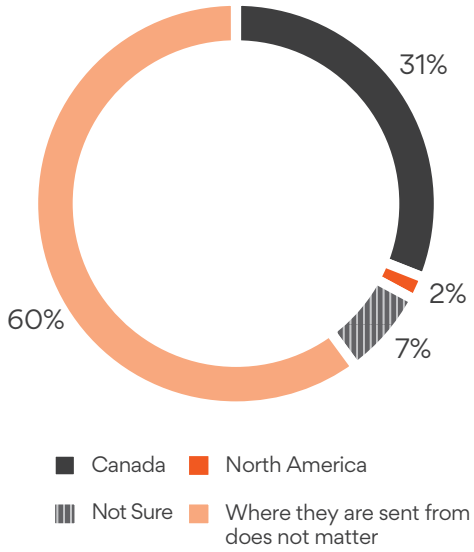
Given the phrasing of section 51 of CASL, it is not clear how a court will determine statutory damages in the range of "up to $200". This raises a number of questions – including the following:

- Would $200 be the default or must certain circumstances be present for the $200 to apply (instead of, say, $5 or $50)?
- Would a court use the statutory damages amount as a proxy for actual (but unproven) damages?
- Would the amount of statutory damages be chosen based on its deterrent effect?
- Would the amount of statutory damages vary depending on whether actual damages were proven?

Although CASL permits both statutory and actual damages, one would think that a court would decline to award statutory damages if the actual damages exceeded $200 per violation. However, it remains to be seen whether courts will impose statutory damages in addition to actual damages.

46% of respondents were unaware that an organization could be liable for statutory damages under CASL, which do not require proof of actual damages.

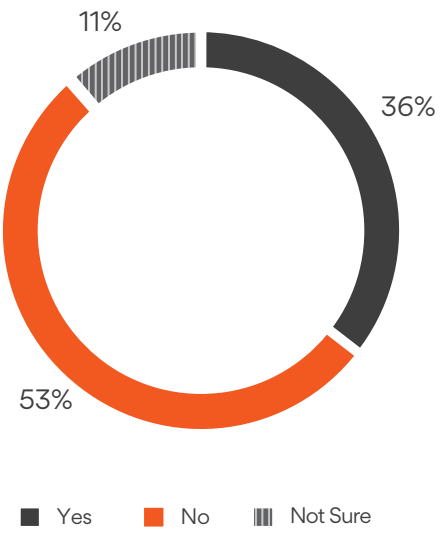
8. CASL only applies to emails sent from:



CASL applies regardless of the senders' jurisdiction. For CASL to apply, the email (or other e-marketing message) must be sent within Canada or sent into Canada. Foreign organizations that send e-marketing messages to Canadian recipients, or organizations that send e-marketing messages within Canada, must comply with CASL. CASL includes an exception for emails sent from Canada to certain jurisdictions (e.g., the US) if the message complies with the equivalent anti-spam law of that jurisdiction.

40% of respondents did not appreciate that CASL applies to messages received in Canada regardless of the jurisdiction from which the message was sent.

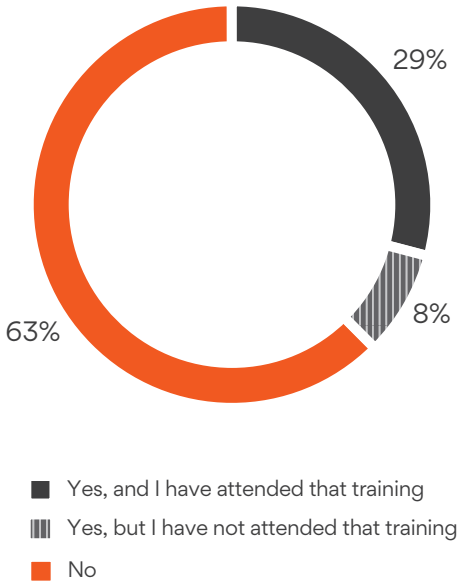
9. **Does your organization have a formal, written CASL policy?**



CASL does not require that organizations adopt a formal written CASL policy; however, the CRTC expects organizations to have implemented one (see CRTC guidance materials). Such a policy will evidence an organization's compliance standards and its efforts to ensure a consistent approach to compliance throughout the organization. This makes having a CASL policy an important element of any due diligence defence in the event of CASL non-compliance (whether as a defence raised by the organization, or by its directors or officers in defending themselves against personal liability).

64% of respondents stated that their organizations did not have (or they did not know if they had) a formal written CASL policy.

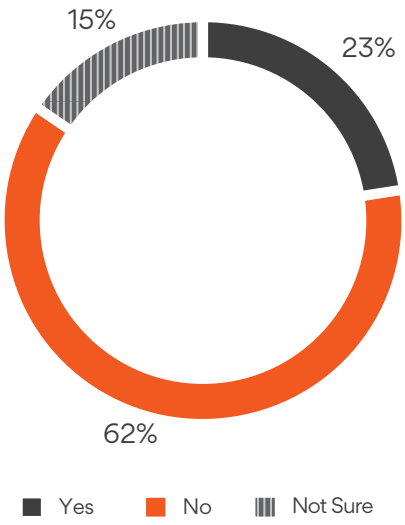
10. **Does your organization require personnel to attend training to understand your organization's CASL policy and how your organization is managing e-marketing messages according to CASL?**



CASL does not require that organizations conduct personnel training; however, the CRTC expects organizations to have implemented a CASL compliance program that includes training (see CRTC guidance materials). That training could vary based on the degree to which personnel are involved in CASL-related activities (such as collecting consent, sending messages, or processing complaints or unsubscribe requests). Without such training, an organization would have more difficulty establishing that it took appropriate steps to ensure compliance throughout the organization. In this regard, CASL training can be an important element of any due diligence defence in the event of CASL non-compliance (whether as a defence raised by the organization, or by its directors or officers in defending themselves against personal liability).

63% of respondents stated that their organization does not require personnel to undergo CASL training.

11. **Has your organization used e-marketing list(s) containing addresses compiled by third parties?**

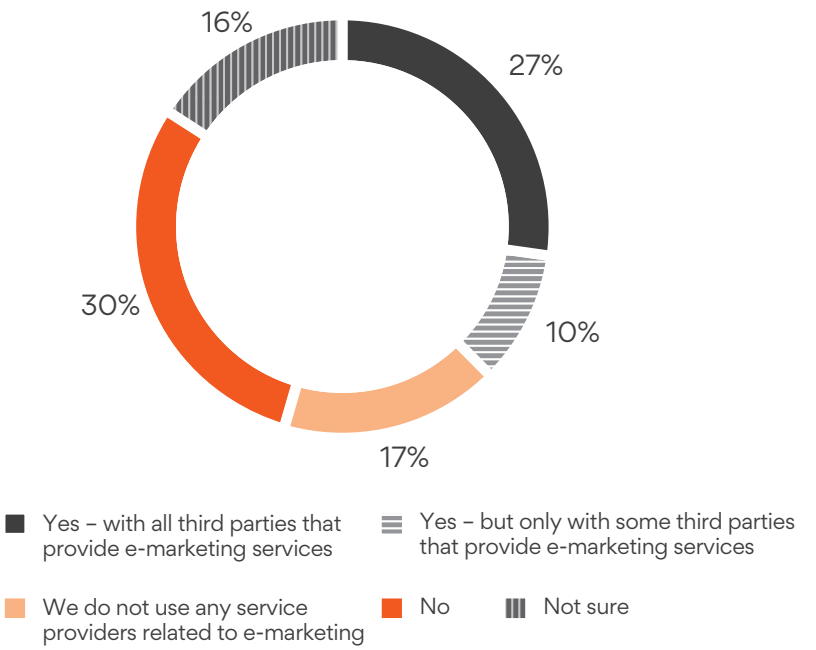


Under CASL, organizations are responsible for ensuring that the e-marketing messages they send (or that are sent on their behalf) comply with CASL. Organizations are also responsible for any CASL violation committed by their agents and mandataries.

Organizations that rely on a third party to compile addresses for e-marketing purposes do so at some risk – namely, that there is no basis under CASL to send e-marketing messages to those addresses, or that the basis is not sufficiently documented. Such organizations should ensure that their contracts with those third parties address CASL compliance and permit effective recovery for any CASL breach. Also, prior to engaging third parties, and periodically during their engagement, organizations should take steps to review how those third parties comply with CASL (in practice) – and not merely rely on contractual clauses.

23% of respondents indicated that their organizations relied on third party e-marketing lists. As a result, these organizations face an additional layer of compliance complexity and are exposed to greater risk of liability.

12. Does your organization have written contracts with third parties who provide e-marketing services (e.g., collecting addresses, designing messages, sending messages, processing unsubscribe requests)?



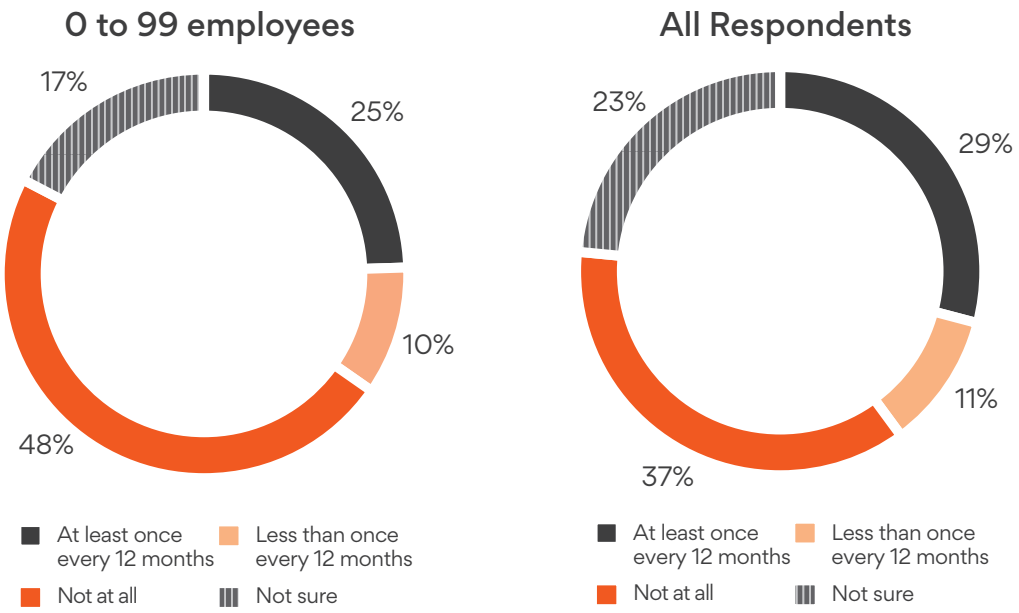
Outsourcing e-marketing services inherently involves the risk of CASL non-compliance, given that an organization can held responsible for a CASL violation caused by a service provider.

Because of this, outsourcing any e-marketing functions should be done pursuant to a written contract. That contract should have appropriate clauses to address CASL, including a requirement to comply with those aspects of CASL that are relevant to each party, to be responsible for any breaches of those requirements (e.g., by an indemnity), and to have appropriate carve-outs from any limitations on liability. Without a written agreement that clearly addresses CASL compliance, organizations may have no recourse against their service providers, and service providers may have no recourse against their clients.

Written contracts are also an important element of any due diligence defence in the event of CASL non-compliance (whether as a defence raised by the organization, or by its directors or officers in defending themselves against personal liability).

40% of respondents indicated that they do not have contracts in place with each of their e-marketing service providers.

13. How often does your organization audit its compliance with CASL?



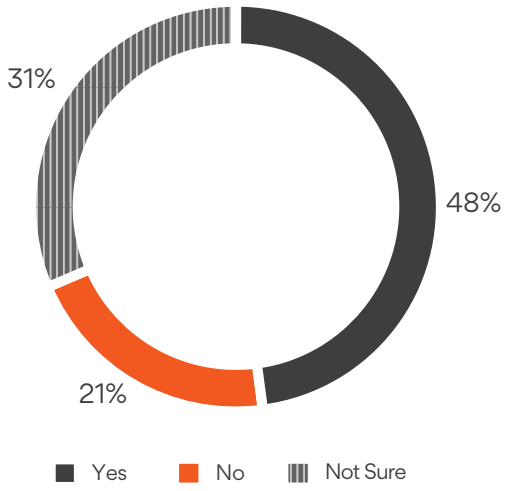
CASL does not require organizations to conduct compliance audits. However, the CRTC expects organizations to conduct periodic compliance audits as part of their CASL compliance program. These audits would assess ongoing compliance (and potentially mitigate or minimize incidents of non-compliance) and should encompass both an organization's own CASL-related activities and those of its e-marketing service providers.

In addition, periodic audits are an important element of any due diligence defence in the event of CASL non-compliance (whether as a defence raised by the organization, or by its directors or officers in defending themselves from personal liability).

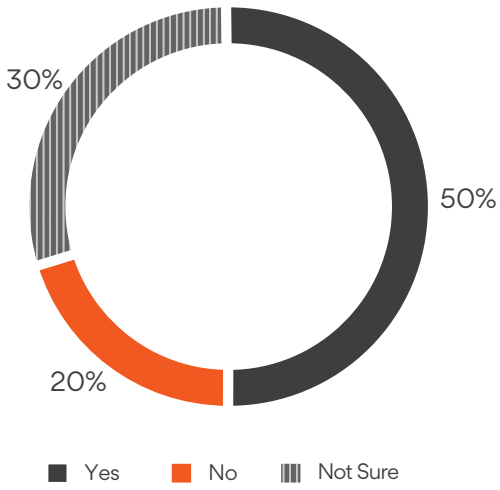
Smaller organizations are more likely to fall short of this important compliance measure: 48% of respondents at organizations employing less than 100 employees do not conduct these audits and 17% are unaware of whether their organization conducts CASL audits.

60% of respondents indicated that their organization does not audit CASL compliance or were unsure.

14. Could your organization prove (with supporting documentation) that it has the authority under CASL to send every e-marketing message sent by your organization (e.g., express consent, implied consent or an exception to consent)?

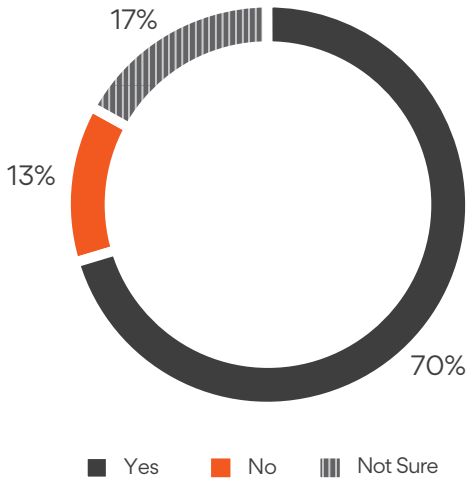


15. Could your organization prove (with supporting documentation) that every e-marketing message sent by your organization includes the specific message content required by CASL?



Only 48% and 50% of respondents were confident about their organizations' ability to evidence compliance with the consent and content requirements, respectively.

16. **Could your organization prove (with supporting documentation) that every e-marketing message sent by your organization includes an easy to use unsubscribe mechanism?**



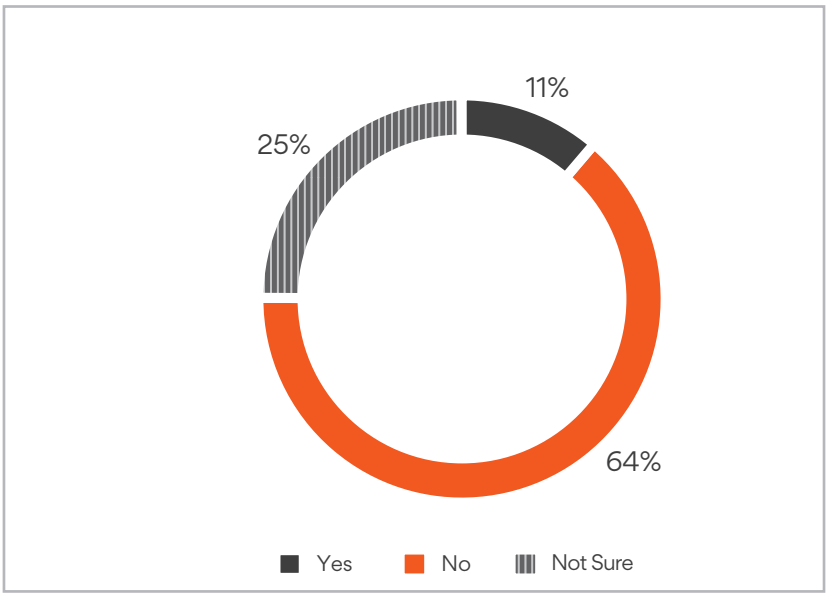
CASL requires organizations to be able to prove that, for every e-marketing message they send (or is sent on their behalf):

- They have the authority to send it
- The message includes the content prescribed by CASL
- The message includes an easy to use unsubscribe mechanism

Proving these elements can be challenging. It requires organizations to be able to implement audit trails to track who was sent a message, when the message was sent, and what the message contained. It also requires organizations to be able to demonstrate the specific authority under CASL under which the message was sent. As examples:

- If the basis is express consent, the organization must be able to prove when and how that express consent was obtained from the recipient
- If the basis is implied consent, the organization must be able to prove how and when that implied consent arose (to establish that it has not expired)

17. **Has your organization received any communication from a non-governmental organization that is voluntarily policing or otherwise promoting compliance with anti-spam laws?**



The CRTC, the Competition Bureau and the Privacy Commissioner of Canada are not the only relevant actors in enforcing CASL. Non-governmental organizations are voluntarily policing compliance with CASL (including offering services to recipients to manage or block unwanted CEMs). These organizations have taken an active role in communicating directly with organizations regarding actual or perceived non-compliance with CASL. Aside from suggesting how an organization can address actual or perceived non-compliance, these organizations also initiate complaints and may provide information directly to regulators to assist them in enforcing CASL.

Organizations who have made a risk calculation on the basis that their clients and potential clients (as email recipients) would not initiate complaints may find that those calculations have not accounted for these independent actors.

Authors

Andrew S. Nunes
Partner, Fasken
+1 416 865 4510
anunes@fasken.com

Daniel Fabiano
Partner, Fasken
+1 416 868 3364
dfabiano@fasken.com

Derek Lackey
President, Direct Marketing
Association of Canada (DMAC)
+1 416 524 7844
derek.lackey@directmac.org

Contributors

Alex Cameron
Partner, Fasken
+1 416 865 4505
acameron@fasken.com

John P. Beardwood
Partner, Fasken
+1 416 868 3490
jbeardwood@fasken.com

Leslie Milton
Partner, Fasken
+1 613 236 3882
lmilton@fasken.com

FASKEN