Best Practices for Canadian Application-to-Person (A2P) Messaging Programs

Version 1.0

August 2023

Canadian Telecommunications Association

Table of contents

1. About this guide 3

1.1 Key takeaways 3

1.2 Association member commitments 5

2. About A2P messaging 5

2.1 A2P messaging channels and protocols 6

2.2 Types of A2P programs 7

3. Best practices and recommended standards 8

3.1 Consent 8

3.1.1 Opt-in: Express consent 8
3.1.2 Opt-in: Implied consent 8
3.1.3 Consent records 9
3.1.4 Transferring consent 9
3.1.5 Confirmation or welcome message 10
3.1.6 Double-opt-in or handset verifier for subscription programs 10
3.1.7 Opt-out 10

3.2 Program management standards 11

3.2.1 Customer support keywords 11
3.2.2 Embedded URLs 3
3.2.3 Quiet hours 3
3.2.4 Transferring subscriber lists 3
3.2.5 Character limit 3

3.3 Promotion and advertising 4

3.3.1 Program pricing 4
3.3.2 Terms and conditions 5

3.4 Program testing and auditing 5

3.4.1 Pre- and post-launch testing 5
3.4.2 Ongoing compliance audits 5

3.5 Spam and malicious messaging 6

3.6 Discouraged A2P sending and business practices 6

3.6.1 Grey route messaging 6
3.6.2 Number sharing 6
3.6.3 Number/URL cycling 7
3.6.4 Snowshoe messaging 7
3.6.5 Artificial traffic inflation fraud 7
3.6.6 Spoofing 7
3.6.7 Spam, phishing and malicious messaging 7

3.7 Special use cases 7

3.7.1 Age-restricted content 7
3.7.2 Political messaging 8
3.7.3 Time-sensitive and critical communications 8
3.7.4 Purchased debt collection 8
3.7.5 Aliases and proxy numbers 9
3.7.6 Text-to-buy (payment authorization) 9

3.8 Consumer compliance and data governance 9
3.8.1 Personal identifiable information 9
3.8.2 Security assessment and authorization audits 10
3.8.3 Organizational compliance policies 11
4. Advice to share with end users 11
Appendix A: Common terms, definitions, and protocols 12
Appendix B: Common A2P use cases 15
Appendix C: Messaging protocols 17
Appendix D: A2P messaging channels 18
Appendix E: Regulatory resources 27

Legal disclaimer:

This guidance document is provided by the Canadian Telecommunications Association ("the Association") for information and guidance purposes only. The Association does not make any representations or warranties regarding the accuracy, timeliness, completeness, sufficiency, or suitability of the information in this document for any particular purpose. The information provided herein is provided "as is", and the Association is under no obligation to update, correct or retract the information in this document, or to publish a new document to reflect any new or additional information that comes to light after this document is first published. The Association does not assume any responsibility or liability for any consequences arising out of the use of any information contained in this document, including without limitation, any and all losses, liabilities, damages, actions, suits, claims or demands. If any recipients of this document use any information contained herein, they do so at their own discretion. The Association strongly encourages all recipients of this document to conduct their own due diligence and obtain independent legal advice on the information contained in this document. In the event of any inconsistency between the information in this document and any applicable laws or regulations, the Association encourages recipients to follow the applicable laws and regulations, which prevail at all times. Nothing contained herein confirms any legal compliance. It is the responsibility of the content provider to comply with all applicable laws and regulations.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

1. About this guide

Application-to-person (A2P) messages are those sent to end users by or through a business or service platform. A2P programs can be used to deliver a variety of message types and content, including suspected fraud alerts, payment reminders, delivery notifications, surveys, promotional alerts, and more. Organizations involved in the operation of A2P messaging programs in Canada must abide by all applicable laws, rules and regulations that govern the delivery of these types of messages, including Canada's Anti-Spam Legislation and applicable privacy laws.

This guide is equally applicable to P2A (person-to-application) messages and programs.

The Canadian Telecommunications Association[1] ("the Association") has developed this guide on A2P messaging best practices and recommended program standards to:

- Provide direction and recommendations to content providers, brands, aggregators, and application service providers (ASPs) on how to effectively manage A2P programs in Canada
- Advocate for the protection of end users by reducing spam and other malicious messages
- Facilitate the continued growth and adoption of A2P messaging in Canada by ensuring it continues to be seen as a trusted communications channel by end users

Given its role as the authority on wireless issues and trends in Canada, industry stakeholders requested that the Association lead the development of this guide. Association members represent companies that provide services and products across the wireless sector, such as mobile network operators (also called wireless carriers), aggregators, and ASPs. By representing the industry before all levels of government and various regulatory agencies, the Association actively nurtures the continued growth of the wireless sector in Canada.

1.1 Key takeaways

The following are best practices and recommended standards for A2P messaging programs in Canada:

1. All programs should be consent-based before any messages are sent. Sending unsolicited messages or spam should be strictly avoided.

2. All programs should provide an opt-out mechanism using STOP/ARRET. Examples of other opt-out commands that should be respected include CANCEL, UNSUBSCRIBE, QUIT, and END.

3. Programs should not use deceptive or misleading promotion/advertising to gain participation.

4. All messages sent to an end user should accurately identify the A2P number and the brand/organization from which the message was sent (or sent on behalf of).

5. All programs should send responses to the following five mandatory keywords:

[1] The Canadian Telecommunications Association was formerly named the Canadian Wireless Telecommunications Association.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

- **HELP:** Identify the message sender or program name, customer support information, price, and opt-out information. Texting HELP should return an English[2] response.
- **AIDE:** Identify the message sender or program name, customer support information, price, and opt-out information. Texting AIDE should return a French response.
- **INFO:** Identify the message sender or program name and customer support information. Texting INFO should return a bilingual response.
- **STOP:** Immediately opt the user out of receiving any further messages. Texting STOP should return an English response[3].
- **ARRET:** Immediately opt the user out of receiving any further messages. Texting ARRET should return a French response.

6. Due to their administrative nature, mandatory keywords should not exceed a single message segment or 160 characters, whichever is shorter.

7. End users should be informed of the cost of participating in an A2P program (e.g., "std msg rates may apply"). In cases where the end user receives a mobile terminating (MT) message containing a clickable link to a website, the content of the message containing the link should state that "data rates may apply." (Stating "std msg & data rates may apply" is equally appropriate.)

8. If programs involve time-sensitive information (e.g., news, stocks, event, or sports score updates) or urgent/critical communications, produced timestamps should be included in each message.

9. An urgent/critical communications program should not be advertised or promoted using the word "emergency".

10. Programs involving age-restricted content such as alcohol, tobacco, cannabis, gambling, or other mature content (e.g., nudity) should verify that each user is of legal age in their province or territory before participating in the program.

11. Programs should not send content related to hate speech, profanity, depictions and endorsements of violence, or any unlawful content.

12. To protect the integrity of the channel, it is recommended that A2P messages not exceed 320 characters or two message-segments, whichever is shorter.

For more information on each of these key principles, see the "Best practices and recommended standards" section of this guide.

[2] Subject to any applicable language laws.
[3] Subject to any applicable language laws.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

1.2 Association member commitments

This guide and the best practices and recommendations within have been developed by the Association in consultation with its wireless carrier, aggregator and application service provider members as the preferred operating standards for A2P messaging programs in Canada.

While the Association does not have the authority to enforce this guide and the best practices outlined within, other than as it relates to Canadian Common Short Codes, organizations involved in the Canadian A2P messaging ecosystem are strongly encouraged to adhere to these best practices and recommended program standards to ensure that A2P messaging in Canada continues to be seen as a trusted communications channel by end users.

2. About A2P messaging

Application-to-person (A2P) messaging refers to messages that are sent by or through a business or service platform that is connected directly to an aggregator or wireless carrier. Essentially, they are any messages sent to end users (or consumers) by businesses in Canada. They can include appointment reminders, delivery notifications, payment reminders, surveys, and many other types of alerts and informational or promotional messages. A2P messaging is different than person-to-person (P2P) messaging (also called peer-to-peer messaging), which is when two or more people communicate by text using their own mobile devices.

A2P messaging	P2P messaging
• Large, medium, or small businesses text multiple customers simultaneously or in bulk • Communications may be between customers and call centres or other customer service/support scenarios • Types of messages include recurring alerts, informational notifications, one-time passwords, and two-factor authentication (2FA) • Also includes marketing messages that promote a product or service	• An active subscriber of a wireless carrier texts another person • The message author is identified by a valid phone number associated with a wireless carrier on a mobile device • The message is composed by the person within a supported messaging client installed on a mobile device • Messages between the author and the recipient(s) have the potential to be two-way, interactive communications

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

2.1 A2P messaging channels and protocols

Messaging channels and protocols are the foundation of how A2P messaging works. In July 2003, Canada's wireless carriers came together with the Assocaition to offer Common Short Codes to be activated across mobile networks. The A2P messaging ecosystem has continued to evolve within the Canadian market since then and now includes the following channels:

- **Common Short Codes (CSC):** A three- to six-digit number that replaces a traditional telephone number to send text or multimedia messages to a mobile device.
- **Toll-free numbers:** A 10-digit text-enabled toll-free phone number used to send text or multimedia messages to a mobile device.
- **10-digit long codes (10DLC):** A 10-digit text-enabled landline phone number used to send text or multimedia messages to a mobile device.
- **Rich business messaging (RBM):** A communication channel between wireless carriers and compatible Android devices that uses data or Wi-Fi to provide enhanced messaging between businesses and end users.

Role of the Association

While the Association is responsible for administering Common Short Codes in Canada, it is not responsible for ensuring compliance of non-CSC A2P programs such as 10DLC, toll-free numbers or RBM. The Association encourages organizations involved in A2P messaging to adhere to these best practices This will help protect Canadian consumers from unwanted messages and spam.

Standardized messaging protocols are what allow brands and content providers to exchange data and connect to end users through these A2P channels. Each messaging channel can be used across multiple protocols, which include:

- **Short messaging service (SMS):** A communication standard for mobile messaging systems that enables sending text-based messages between mobile devices.
- **Multimedia messaging service (MMS):** A communication standard for mobile messaging systems that enables sending multimedia messages (such as images and video files) between mobile devices.
- **Rich communication services (RCS):** A communication standard for compatible Android devices that enables sending messages between mobile devices using rich and enhanced features such as delivery and read receipts.

For the full list of common A2P use cases and how-to-guides for implementing them according to the best practices outlined in this guide, see Appendix B. For more information about A2P messaging channels and protocols, see Appendix C and Appendix D.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

2.2 Types of A2P programs

All A2P programs fit into a program category and can be further classified by a specific use case. The following categories are based on intended use, frequency or ratio of interactions, and consent type to be expected.

	Informational	Conversational	Promotional
Intent	Program sends alerts to end users (either recurring or one-time) based on a specific event, service, or account.	Program and end user engage in equal back-and-forth, chat-like communication.	Program promotes a brand, product, or service to encourage participation in a commercial activity.
Frequency	End users can expect either a single message sent and received or are expecting multiple messages connected to a specific event. The request for information may be by mobile originating (MO) keyword or by providing a mobile number to receive single or multiple messages, depending on the use case.	End user provides their contact details to an organization and requests to be contacted. End user engages with a program by MO keyword or by providing their number to converse with a person, agent, customer service representative, or bot. A ratio of one MO message to one mobile terminating (MT) message is expected.	Messages are sent to an end user that contains a sale, marketing promotion, coupon code, or discount to encourage participation in commercial activity. Messages may be recurring as part of an ongoing subscription program or on-demand.
Consent type	EXPRESS recommended		
	In all scenarios, proof of consent, whether obtained using express or implied through an agreement or contract, should be retained by the brand or content provider.		

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

3. Best practices and recommended standards

This section includes information to help business and organizations manage and deliver a successful A2P program. It covers broadly applicable topics such as consent and program management, as well as specific use cases such as age-restricted content and political messaging. **Nothing contained herein confirms any legal compliance. It is the responsibility of the content provider to comply with all applicable laws and regulations.**

3.1 Consent

Under Canada's Anti-Spam Legislation (CASL), individuals and businesses must obtain CASL-compliant express or impled end user consent before sending commercial electronic messages ("CEMs"), such as emails or texts. (For more information about CASL, visit https://fightspam.gc.ca.)

End userconsent is recommended for all A2P programs, regardless of whether or not they constitute CEMs, and may be revoked or withdrawn at any time by the end user. The sending of A2P messages, without the end user's prior consent, should be strictly avoided.

Regardless of the consent type obtained, the brand or organization that obtains the consent should be the only party that sends a message to a consumer who provided the consent.

3.1.1 Opt-in: Express consent

Express consent is the explicit permission from an end user to be contacted by or to participate in an A2P program. Express consent does not expire; however, the recipient has the right to withdraw their consent at any time. Content must not be delivered until after the consumer has confirmed their desire to participate in an A2P program. Wherever possible, express consent should be obtained. Express consent can be obtained by:

- Providing a mobile number online
- Verbally providing a mobile number and/or consent over the phone
- Texting or tapping to initiate communication with an A2P program
- Providing a mobile number and/or consent in writing on a paper or electronic form

3.1.2 Opt-in: Implied consent

Implied consent is a form of opt-in not explicitly provided by an individual, but implicitly granted by, for example, an end user's existing relationship with a business or through an agreement between the end user and a business (e.g., financial institutions have agreements with all of their customers) that includes language describing that customers can be contacted using the information they have voluntarily provided.

Under CASL, implied consent typically expires after a fixed period of time (e.g., 2 years) unless an intervening event occurs, such as the end user opting-in expressly or opt-out.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

3.1.3 Consent records

Once an end user has volunteered to participate in an A2P program or has been opted-in using implied consent, consent records should be retained by the content provider or brand.

The Canadian Radio-television and Telecommunications Commission (CRTC) has the right to investigate or perform a compliance check; in this case, the content provider will need to produce proof of consent and a copy of the brand or content provider's information management policies.

Good record-keeping practices may help businesses:[4]

- Identify potential non-compliance issues
- Investigate and respond to consumer complaints
- Respond to questions about the business' practices and procedures
- Monitor their corporate compliance program
- Identify the need for corrective actions and demonstrate that these actions were implemented
- Establish a due diligence defence in the event of complaints to the CRTC against the business

Companies should consider maintaining hard copy and/or electronic records of the following:

- Commercial electronic message policies and procedures
- All unsubscribe requests and resulting actions
- All evidence of express consent (e.g., audio recordings, completed forms) from consumers who agree to receive commercial electronic messages
- Commercial electronic message recipient consent logs
- Commercial electronic message scripts
- Commercial electronic message campaign records
- Staff training documents and other business procedures

3.1.4 Transferring consent

Generally speaking, consent is granted by an end user to a brand for a specific use case. For example, an end user agreeing to be sent a two-factor authentication code may not be automatically opted-in to marketing alerts. Similarly, a brand that has collected end user consent may not share that consent with partners, affiliates, or subsidiaries, without the end user's permission.

Transferring consent is appropriate when an acquisition has taken place and the use case remains the same. When consent has been transferred from one organization to another and the overall use case remains the same, the end user should be made aware, but re-opt-in is discretionary. Should the use case change because of an acquisition, re-opt-in should take place.

[4] https://crtc.gc.ca/eng/com500/guide.htm

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

3.1.5 Confirmation or welcome message

Acknowledgement of opt-in should take place. A confirmation, "thank you" or "welcome" message should be sent following an opt-in, regardless of the opt-in method. Best efforts should be made to send opt-in confirmation promptly following the opt-in, ideally within 48 hours.

In instances where opt-in is provided manually (e.g., via a paper form), the confirmation or welcome message should be sent within 30 days.

Example of a confirmation/welcome message for express consent:

> *ABC Airline: You will now receive alerts for upcoming flight A912. To opt-out of flight alerts, text STOP. Std msg rates may apply.*

Example of a confirmation/welcome message for implied consent:

> *Message from YXZ Bank: You have been subscribed to low balance warning alerts under Bill-C86. To opt-out, text STOP. Std msg rates may apply.*

3.1.6 Double-opt-in or handset verifier for subscription programs

In instances where consent is given by the end user to subscribe to recurring alerts using a web-based, manually entered, written, or verbal opt-in, the use of a handset verifier (or double opt-in) is recommended. A handset verifier allows the content provider to positively confirm that the authorized subscriber is acknowledging the opt-in. A handset verifier should include:

- The exact instructions for the end user's action (e.g., "To accept reply YES" or "Enter PIN 1234 online to complete subscription")
- Contact details/customer support information for the brand or content provider
- How to opt-out of the program using STOP/ARRET

3.1.7 Opt-out

Consumer consent for an A2P program can be revoked at any time and all involved parties should promptly action every opt-out request.

If an end user opts out of a program, their mobile number should be removed from contact or subscription lists and no further messages should be sent, with the exception of one acknowledgement message that the user has successfully opted-out or unsubscribed.

Additionally:

- A2P programs should promote opt-out keywords STOP and ARRET.
- Other universal opt-out commands should be recognized, such as END, CANCEL, UNSUBSCRIBE, QUIT or FIN, ANNULER, QUITTER, DESABONNER in French.
- Opt-out via a URL, online account, call centre, or paper form should also be accepted. These opt-out methods should be in addition to supporting STOP/ARRET.
- An end user should be able to opt back into a program at their discretion and should not be blocked/blacklisted from the A2P program after texting an opt-out keyword.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

3.2 Program management standards

The A2P program standards described below should be used as a guide to promote good messaging practices and a positive user experience.

3.2.1 Customer support keywords

The following five keywords should be implemented for all programs, regardless of price point, intended audience, message frequency or commercial availability:

- STOP
- HELP
- INFO
- ARRET
- AIDE

These five keywords should be:

- Promoted in CAPITAL LETTERS to emphasize importance
- Available in both English and French regardless of the intended audience
- No more than one message segment or 160 characters (as they are administrative in nature)
- Delivered free of charge wherever possible

<table>
<tr><th>Keyword</th><th>Intention</th><th colspan="2">Message content recommendations</th></tr>
<tr><td>HELP</td><td rowspan="2">Should provide the end user with high-level program information and customer support/contact information for the brand or content provider</td><td colspan="2">HELP should generate an English[5] response that includes:
Program name or brand name
Contact information for the brand or content provider (email, URL and/or phone number)
Cost
Message frequency of the program, if a subscription
Opt-out/unsubscribe information using STOP</td></tr>
<tr><td>Example non-subscription response:
ABC Transit Info: Questions or info? Visit: https://abctransit.ca. Text STOP to cancel. StdMsg&DataRatesApply</td><td>Example subscription response:
XYZ Loyalty Programs: Up to 2 msgs/week. For help, email support@abc.com. Std msg rates may apply. Reply STOP to cancel.</td></tr>
<tr><td>AIDE</td><td colspan="2">AIDE should generate a French response including the following:
Program name or brand name
Contact information for the brand or content provider (email, URL and/or phone number)
Cost
Message frequency of the program, if a subscription</td></tr>
</table>

[5] Subject to any applicable language laws.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

<table>
<tr><th>Keyword</th><th>Intention</th><th colspan="2">Message content recommendations</th></tr>
<tr><td></td><td></td><td colspan="2">• Opt-out/unsubscribe information using ARRET</td></tr>
<tr><td></td><td></td><td>Example non-subscription response:
Service de transport ABC: Questions ou info? Visitez https://abctransot.ca Répondez ARRET pour annuler. FraisStdDeMsg&DonnéesPeuvS’appl</td><td>Example subscription response:
Promos de XYZ: Jusqu’a 2 msgs/sem. Pour de l’aide: soutien@abc.com Frais std de msgs s’applique. Répondez ARRET pour désabonner.</td></tr>
<tr><td>INFO</td><td rowspan="3">Should provide the end user with brand/program name and customer support information</td><td colspan="2">INFO should generate a bilingual response including the following:
• Program name or brand name
• Contact information for the brand or content provider (email, URL and/or phone number)</td></tr>
<tr><td>Example non-subscription response:
ABC Transit Info: Have questions or need assistance? Call 1-800-555-5555 | Info de transport ABC: Questions ou besoin de l’aide? Appelez 1-800-555-5555</td><td>Example subscription response:
XYZ Loyalty Promotions: Have questions or need assistance? Call 1-800-555-5555 | Promotions de XYZ: Questions ou besoin de l’aide? Appelez 1-800-555-5555</td></tr>
<tr><td>STOP</td><td colspan="2">STOP should generate an English response[6] indicating:
• The user will receive no further messages
• For non-subscription services (one-time use, such as 2FA), send one message stating that the service is not a subscription and the consumer will receive no further messages</td></tr>
<tr><td rowspan="3"></td><td>Example non-subscription response:
ABC Transit Info: This is not a subscription service. You will not receive any further messages.</td><td>Example subscription response:
XYZ Loyalty Programs: You have successfully unsubscribed and will not receive any further messages.</td></tr>
<tr><td>ARRET</td><td colspan="2">ARRET should generate a French response indicating:
• The user will receive no further messages
• For non-subscription services (one-time use, such as 2FA), send one message stating that the service is not a subscription and the consumer will receive no further messages</td></tr>
<tr><td>Example non-subscription response:
Service de transport ABC: Ceci n'est pas un service d'abonnement. Vous ne recevrez plus de messages.</td><td>Example subscription response:
Promos de XYZ: Vous vous êtes désabonné et ne recevrez plus de messages.</td></tr>
</table>

[6] Subject to any applicable language laws.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

3.2.2 Embedded URLs

Content providers should ensure URLs embedded with a message do not misrepresent the sender's identity and are not malicious or deceptive. Additionally:

- URLs within a message should identify the brand and owner of the website.
- Shortened URLs should be avoided if they do not include the brand or content provider's name. Shortened URLs can look like spam and are more likely to be caught in spam filtering mechanisms.
- Messages that contain a URL should state that "data rates may apply".

3.2.3 Quiet hours

To ensure a positive user experience, it is recommended that messages be sent between 9 a.m. and 9 p.m. only. This applies primarily to marketing messages because informational alerts such as transactional messages, fraud alerts, account recovery/2FA, and appointment reminders should be sent when needed.

3.2.4 Transferring subscriber lists

Only end users that have opted into a program may be transferred to another A2P channel, and the program's content should remain as initially promoted to the consumer. In addition:

- Organizations are permitted to transfer a list of subscribers from one A2P channel to another in instances where the subscribers have opted-in using valid mechanisms.
    - For example, a transfer could occur when an organization has built a subscriber base by obtaining opt-ins on a 10DLC and would like to transfer their subscribers to a dedicated Common Short Code.
- To provide the best possible user experience, organizations should send a single MT to each subscriber from the original number that provides:
    - The identity of the program by company name or organization name
    - A note that the actual number associated with the subscription service will be changing
    - The new number
    - Customer support information

3.2.5 Character limit

To maintain the integrity of the A2P messaging channel, it is recommended that an A2P message not exceed two message segments or 320 characters.

A2P messages should be treated differently than email. A2P messages should be concise and to the point. Unnecessarily long messages are not recommended. Reasonable exceptions to this recommendation include chat/conversational programs and programs that may need to send messages bilingually.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

3.2.6 Scrubbing deactivated numbers

A deactivated number is a number that has been removed from a wireless carrier's network, often as a result of a contract cancellation between the wireless carrier and the customer.

When a wireless carrier deactivates a number, that number will eventually be made available for use by another customer (typically after 90 days). To ensure that number is no longer associated with any A2P programs, aggregators and ASPs should scrub deactivated numbers from their databases.

If deactivation lists are not provided by the wireless carriers directly as a best practice, aggregators, and ASPs should delete any mobile numbers in cases where:

- Text messages have been undeliverable for a period of 30 consecutive days
- It can be determined that the unsuccessful deliveries are due to the number being inactive on the wireless carrier network

3.3 Promotion and advertising

When promoting an A2P program, content providers should ensure advertising is clear and conspicuous regarding all terms and conditions associated with participating in the program. Additionally:

- When a user is asked to provide their mobile number, clear language that is adjacent to the mobile number entry field should clearly disclose that by providing their mobile number, the end user is agreeing to be contacted.
- Content providers should supply links to relevant legal documents (such as terms and conditions and privacy policies) to detail how consent and opt-outs are managed.
- When disclosing pricing and terms, easy-to-understand language and fonts should be used.
- Content providers should not use deceptive or misleading promotion/advertising to gain participation in a program.
- Programs should not be associated with or used to entice users to access content that is associated with any illegal practices such as copyright violations or piracy.
- The program should not be used for the promotion or marketing of any wireless carrier without their explicit permission

3.3.1 Program pricing

At all times, content providers should inform users of the cost of interacting with their program. No program should be promoted as being free until it can genuinely be acquired for free by the end user. In addition:

- If an SMS service costs the consumer a standard rate messaging fee, content providers should disclose that "std msg rates may apply". Content providers may also choose to say "msg rates may apply", "std msg & data rates may apply", or a similar variation to this disclosure.
- In cases where there is an MMS component to a standard rated program, content providers should disclose that "std msg & data rates may apply".

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

- For programs using a data or Wi-Fi connection, content providers should disclose that "data rates may apply".
- Pricing disclosures should be easily visible and adjacent to the call-to-action.
- In cases when a user receives a URL or clickable link to a website, the content of the message that contains the URL should state that "data rates may apply". Content providers may also choose to say "std msg & data rates may apply".

3.3.2 Terms and conditions

The program's terms and conditions (or terms of service) is the agreement between the end user and the organization providing the A2P messaging service. Terms and conditions should provide the terms, rules, and guidelines for using or participating in the A2P program. If an A2P program is being offered in both English and French, the applicable terms and conditions should be available in both languages. Additionally:

- Organizations should maintain and noticeably display a program's terms and conditions so that they can be easily found and read by end users.
- Terms and conditions should clearly describe how the organization may collect, use, and share information from end users.

3.4 Program testing and auditing

It is recommended that all content providers, ASPs, and aggregators implement regular program checks/audits to ensure the promotion, message content, and user experience are compliant. Two types of program audits that should be conducted are pre- and post-launch testing, and ongoing compliance audits.

3.4.1 Pre- and post-launch testing

To ensure the A2P program is operating the way it is intended, end-to-end testing should be conducted before the program becomes commercially available to the public. Once the program has gone to market, additional end-to-end testing is recommended to ensure all program elements meet the defined program requirements and have not been altered since launch.

3.4.2 Ongoing compliance audits

It is recommended that content providers, ASPs, and aggregators conduct regular compliance audits throughout the duration of a campaign or program to ensure ongoing compliance.

Audits should cover the following topics and activities:

- **Advertising:** Do all calls-to-action include the appropriate pricing disclosures and terms?
- **Opt-in:** Do the opt-in mechanism work appropriately (including welcome message, where applicable)? Are opt-in records being maintained?
- **Opt-out:** Do opt-out mechanisms like the STOP keyword still work properly?
- **Customer support keywords:** Are the recommended message elements still included and accurate?
- **Spot check message logs:** Is the use case still in line with how the program initially launched? Are there any changes to report to the appropriate messaging partner (or to the

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

Association in the case of a Common Short Code)? Are opt-out rates in line with the expectation?

3.5 Spam and malicious messaging

All A2P program content providers, ASPs, and aggregators are responsible for ensuring any commercial electronic messages they send, or cause or permit to be sent, fully comply with the requirements of CASL.

Best practices for reducing spam and malicious messaging include the following:

- Implied or express consent should be obtained and consent records retained.
- Involved parties should understand the relevant compliance requirements, legislation, and laws related to sending A2P messages.
- ASPs and aggregators should leverage relevant technologies that prevent spam and malicious messaging, such as filters and blocking mechanisms.
- ASPs and aggregators should implement practices and processes for ongoing monitoring and auditing of programs to ensure best practices are being followed and to intercept any spam or malicious messaging.
- ASPs, aggregators, and wireless carriers should suspend, disconnect or block programs affiliated with spam or malicious messaging.
- All those in the ecosystem should report spam/malicious messaging to the appropriate authorities.

3.6 Discouraged A2P sending and business practices

All those involved in the A2P messaging ecosystem are responsible for upholding messaging best practices to protect end users from spam, malicious messages, or otherwise deceitful, harmful, or unlawful content. A2P messaging practices that negatively affect end users may result in the A2P program being suspended indefinitely by the participating wireless carriers, aggregators, and/or ASPs. Damaging A2P messaging practices erode end user's trust in the Canadian A2P ecosystem.

The following A2P practices are discouraged because they do not align with the expected, intended or recommended use of A2P programs in Canada.

3.6.1 Grey route messaging

An A2P message sent over a P2P network should be strictly avoided since A2P traffic is not intended to run over a P2P network.

3.6.2 Number sharing

As it relates to 10DLCs and toll-free numbers, sharing a single number between multiple organizations is not recommended.

As it relates to CSCs, number sharing may be considered on a case-by-case basis. Please refer to the Canadian Common Short Code Application Guidelines for more details or contact shortcodes@canadatelecoms.ca.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

3.6.3 Number/URL cycling

Applicable to 10DLCs and toll-free numbers only, number cycling is when sender monitors an A2P number for degraded deliverability and regularly switches to a new number to reset their reputation. This sending practice actively works to evade wireless carrier filtering mechanisms and is therefore considered malicious.

3.6.4 Snowshoe messaging

Commonly used by spammers, "snowshoeing" is when a single message sender disperses identical or similar messages across multiple numbers. In doing so, the sender aims to evade wireless carrier filtering mechanisms and avoid per-number rate limits and volume limitations at the carrier level. Adopting this technique often results in messages being blocked and should be strictly avoided.

3.6.5 Artificial traffic inflation fraud

Artificial traffic inflation is when messages are sent to an end user to increase the fees that can be charged to a content provider. In some cases international numbers may be used, causing the end user to be charged a premium rate by their wireless carrier.

3.6.6 Spoofing

"Spoofing" is a technique where message senders change the display number on a text sent via SMS or MMS system, usually for malicious intent. Changing a display number, sender number or sender ID is strictly prohibited. Anyone sending A2P messages must accurately identify themselves.

3.6.7 Spam, phishing and malicious messaging

Includes unsolicited bulk messages, "phishing" messages intended to access private information through deception, other forms of abusive, harmful, malicious, unlawful, or otherwise inappropriate messages.

3.7 Special use cases

The following use cases require special consideration and may include additional program standards or best practices to ensure a positive user experience. Special use cases may be considered on a case-by-case basis.

3.7.1 Age-restricted content

For programs involving age-restricted or mature content, such as alcohol, tobacco, cannabis, gambling, or nudity, content providers should first verify with their ASP or aggregator partner the position of each wireless carrier surrounding this use case.

If advised to proceed, content providers should verify that each end user is of legal age in their province or territory of residence before allowing their participation in the program. All programs involving age-restricted content should have a robust age-verification mechanism in place. Age verification can be achieved in the following ways:

- By using the A2P program (e.g., "Reply YES to confirm that you were born after 01/01/2003 and are 19 years of age or older" or "Reply with your DOB (MM/DD/YYY) to continue")
- If the promotion of the program is limited to age-verified locations such as a bar
- If the webpage itself is age-gated

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

3.7.2 Political messaging

A political messaging program is expected to involve:

- Solicitation of support of political candidates
- Information regarding a particular candidate's platform or goals if elected
- Donation solicitation or donation facilitation

All recommended best practices within this document should be considered when running a political messaging program, and users should be providing informed consent to receive political messages. Messages that are libelous, defamatory, or not in full compliance with applicable laws should be strictly avoided. Messages that contain hate, violent or racist rhetoric or symbols, or material reasonably expected to be offensive to a user, without regard to ideological or partisan content, should also be strictly avoided.

A2P opt-in and opt-out consent rules apply, so sharing of lists is not recommended.

3.7.3 Time-sensitive and critical communications

Time-sensitive notifications and critical communications, such as breaking news, stocks, or urgent safety-related alerts, should be administered with careful consideration as message delivery cannot be guaranteed.

When sending these types of notifications:

- Each message should include a timestamp
- Language should be included at the point of opt-in, or in the terms and conditions, to inform the end user that message delivery cannot be guaranteed

In addition, time-sensitive and critical communications A2P programs should:

- Not be used to send "Broadcast Immediate" alerts.
- Not be advertised using the word "emergency" so as to not to be confused with Canada's wireless public alerting system.
- Not be the only method of alerting the community; a secondary method of communication (e.g., email, push notification, voice) should be obtained at the time of opt-in.
- State in their terms and conditions that alerts sent over the wireless public alerting system are to take precedence over any notifications sent via A2P message.

3.7.4 Purchased debt collection

Purchased debt collection is considered debt that has been sold from the original creditor to a third party that is now trying to collect from an end user with whom there is no pre-existing relationship.

For this type of program, content providers should first verify with their ASP or aggregator partner the position of each wireless carrier surrounding this use case. If advised to proceed, content providers should:

- Be informed of each province's debt collection regulations, including contact expectations
- Inform the end user who they are and who the original creditor is
- Provide a phone number, email or URL that can be vetted and validated online

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

3.7.5 Aliases and proxy numbers

In some cases, a content provider may need to mask the sender ID of an A2P number to protect the identity and privacy of the message sender. This is applicable to 10DLCs and toll-free numbers only. For example:

- A food delivery service may need to converse with an order recipient to confirm location.
    - The proxy or alias telephone number acts as a bridge, allowing the delivery person and order recipient to communicate without having to reveal their telephone number.
- A call centre with an established 1-800 number capable of transmitting calls or messages to several other telephone numbers held by the call centre.

3.7.6 Text-to-buy (payment authorization)

For programs involving a purchase or payment authorized via A2P message, content providers should first verify with their ASP or aggregator partner the position of each wireless carrier surrounding this use case.

Text-to-buy is commonly paired with another use case, such as cart abandonment or a mobile marketing subscription, whereby the end user receives a marketing alert or a reminder that they have unpurchased items in their online cart. The end user is then prompted to reply with a specific keyword to initiate or complete the purchase via credit card. It is expected that:

- The credit card details of the end user have been previously provided and are stored securely within the e-commerce website or platform, and the A2P program is used to facilitate the completion of the purchase.
- Credit card information is never requested or sent via the A2P program.
- The text-to-buy message will reference the last four-digits of the end user's credit card.

An example of a text-to-buy message:

> *ABC Clothing: You're almost there! You have 2 items in your cart waiting for you! To complete your purchase using card ending in 1234, reply with CONFIRM or click here: https://ABCclothingURL.ca Data rates may apply. Reply STOP to cancel.*

3.8 Consumer compliance and data governance

These topics offer an overview of Canada's consumer compliance and data governance requirements.

None of this information confirms any legal compliance. It is the responsibility of the message sender to comply with all applicable laws and regulations for A2P programs. To confirm they adhere to all municipal, provincial, and national laws, organizations should further research these topics or seek professional counsel.

3.8.1 Personal identifiable information

All A2P programs involve the collection and retention of certain end user data. Specifically, a mobile number, combined with secondary data points such as postal code, address, and last name, all constitute personal identifiable information (PII). As such, that information is governed under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and Canada's Digital Charter: Trust in a digital world.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

The following best practices apply to PII:

- Businesses/organizations and end users should be aware that PII data may travel across several parties involved in processing the messages.
- Personal security breaches damage end user confidence in A2P programs. Organizations should therefore make their best reasonable effort concerning data protection and security.
- Organizations should obey all relevant regulations and laws governing end users' data privacy and security.

In addition, businesses and organizations leveraging A2P messaging should ensure PII is stored in and accessed from inside Canada only. They should also protect PII by planning security arrangements against risks such as unauthorized access, collection, use disclosure or disposal. Specifically, organizations should:

- Train employees on their roles and responsibilities in protecting PII
- Implement procedures for destroying, erasing, or anonymizing PII
- Develop guidelines and implement procedures for the retention of PII
- Conduct scheduled reviews to determine whether the information is still required
- Establish a data retention schedule

3.8.2 Security assessment and authorization audits

Different types of organizations are held to varying standards in Canada. For organizations that keep PII or are in a regulated industry such as financial services, retail, banking, healthcare, or government, compliance audits are recommended to both safeguard the security of end user's data and to ensure the organization meets required compliance standards.

There are four common types of security assessments:

- **Assessment over risk:** Supports an organization's ability to identify, estimate, and prioritize risk.
- **Vulnerability testing:** Can expose faults in the security protocols, architecture, execution, or internal controls.
- **Test penetration:** Identifies weak points that could be exploited to penetrate an organization's network.
- **Audit of compliance policies:** Determines whether an organization adheres to legal requirements and is not inadvertently exposing its end users' data to risks.

More information on security assessment and authorization audits is available from the Government of Canada.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

3.8.3 Organizational compliance policies

Organizations implement compliance policies to make sure they are compliant with all associated regulations. A compliance program forms the basis for meeting all reporting, record keeping, client identification, and other know-your-client (KYC) requirements.

Best practices for implementing compliance policies include the following:

- Appoint a compliance officer responsible for implementing the program.
- Implement written compliance policies and procedures that are kept up to date.
- Conduct regular risk assessments to assess and document potential risks.
- Implement a written, ongoing compliance training program for employees or other authorized persons, including a regular cadence for the training program.
- Introduce a documented plan to review the compliance program to test its completeness and usefulness. It is recommended to perform this review every two years at minimum.

More information on compliance policies is available from the Competition Bureau Canada.

4. Advice to share with end users

Discouraged and unfavourable messaging practices erode trust in the Canadian A2P messaging ecosystem. This negatively affects all those involved — from the wireless carrier to the end user. Involved parties should work together to promote and uphold the messaging best practices outlined in this document. Only by working collaboratively can the stakeholders in the A2P messaging ecosystem build confidence with Canadian end users and establish A2P messaging as a trustworthy channel.

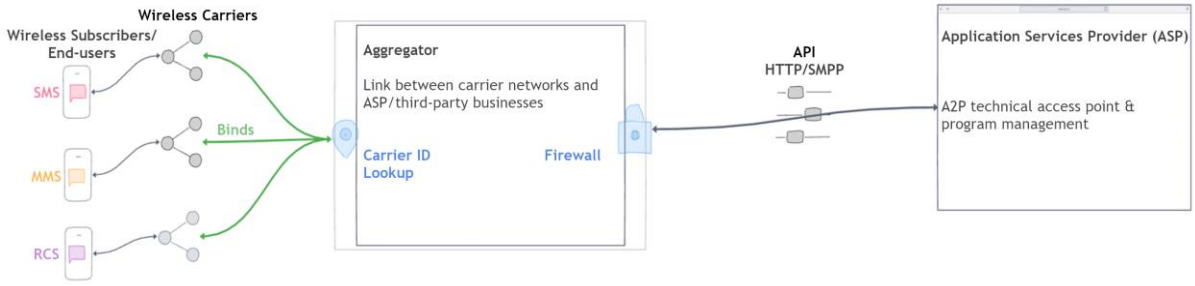
End users also have a role to play. They can take steps to protect themselves from spam and malicious messaging by following these tips:

- Carefully consider the message sender before replying or clicking a link. As a rule of thumb, end users should not engage if they weren't expecting the message.
- Check for misspelled words or other typos to help determine the validity of the message.
- Block suspected spam numbers using the options available on their devices.
- Download trusted spam reporting tools and apps.
- Report the spam message to wireless carriers by forwarding the message to 7726.
- Report spam to the Government of Canada (https://fightspam.gc.ca), which will aid in the enforcement of CASL.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

Appendix A: Common terms, definitions, and protocols

A2P messaging ecosystem: The applications and systems required to send and receive A2P messages from a brand or content provider to an end user. In some instances, an organization can play multiple roles in the A2P messaging ecosystem.



Aggregators: Directly connect to a wireless carrier network to receive/deliver A2P messages.

Application programming interface (API): A software in-between that permits two applications to interact with each other. Two popular APIs in A2P messaging protocols are HTTP(s) and SMPP:

- **Hypertext transfer protocol secure (HTTPS):** Used for protected communication over an application network. The protocol is encrypted to provide authentication, privacy, and data integrity between two applications. Requires firewall for safety.
- **Short message peer-to-peer (SMPP):** An open, industry-standard protocol intended to deliver a flexible data communication interface for data transmission between two applications.

Application service providers (ASPs): Provide messaging software solutions to the content provider.

Brand: The company, business or organization that is engaging with the end user either directly or via a third-party messaging partner. The brand is the public-facing company associated with the A2P program.

Call-to-action (CTA): Marketing collateral or promotional material intended to encourage an end user to engage with an A2P program. Typically the first step in an interaction between an end user and an A2P program.

Carrier ID lookup: A service that provides up-to-date data on a mobile subscriber's wireless carrier affiliation and differentiates between a landline and a mobile number.

Channels: Messaging products within a specific protocol (e.g., Common Short Code, 10-digit long code).

Content providers: Supply the content of the message. Often the public-facing brand behind the A2P program.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

Encoding: The process of converting data from one form to another. Messaging encoding is how text messages are sent to wireless carriers. The type of encoding used involves different types of special characters and the overall number of characters in each segment. Two prevalent types of messaging encoding are UCS-2 and GSM-7:

- **UCS-2 encoding:** Uses 16 bits per character and the segment is limited to 70 characters maximum.
- **GSM-7 encoding:** Uses 7 bits per character and is most common. Allows more than 130 letters and symbols. The segment is limited to 160 characters maximum.

End user: The individual using a mobile device to interact with a business, brand, or organization via an A2P program.

Firewall: A network security system that controls traffic based on set rules (i.e., whitelisting "safe" IP addresses/users).

Multimedia messaging service (MMS): A standard for mobile messaging systems that enable sending of multimedia image-based messages, such as images, audio, and video files.

Mobile originating (MO): A message sent by the end user.

Mobile terminating (MT): A message received by or sent to the end user.

Phishing/smishing: The fraudulent sending of messages to end users to collect personal information, such as passwords and credit card numbers, through deceptive means. "Smishing" is phishing carried out through SMS.

Program(s): An A2P messaging experience offered by a brand or content provider that transmits messages between wireless carriers and end users.

Protocols: Messaging protocols define a standard way for applications to exchange data (i.e., MMS, SMS, RCS).

Rich business messaging (RBM): A communication protocol between wireless carriers and applicable Android devices that uses data or Wi-Fi to provide enhanced messaging (including video and image files) between businesses and end users.

Rich communication service (RCS): A standard supported on compatible Android handsets that facilitates sending messages with enhanced features.

Sender ID: The displayed number or name that appears on a mobile device when a message is received.

Short messaging service (SMS): A standard for mobile messaging systems that enables sending text-based messages.

Spam: The sending of unsolicited messages to an end user that has not provided consent.

Throughput: The measure of data transfer between the connections measured by transactions per second (TPS) or messages per second (MPS).

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

Wireless carriers: Companies that provide access to wireless communications services, such as SMS, MMS, and RCS to their customer, the end user.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

Appendix B: Common A2P use cases

These use cases are common A2P program types that can be used independently or used in conjunction with one another. This is not an exhaustive list but is meant to capture use cases that are most commonly used in the A2P space.

Two-factor authentication (2FA): One-time message containing a PIN or one-time password for identity validation.

Appointment reminders: Reminder notifications about an upcoming scheduled appointment.

Banking alerts: Used to inform end users of completed transactions, to provide low-balance warning or to advise of a purchase threshold reached.

Cart abandonment: Reminder notifications about unpurchased items in an online shopping cart.

Charitable giving: Used to facilitate donations by credit card to charitable organizations, non-profits, or political parties. For information on wireless carrier-billed donations via a Common Short Code, please contact the Mobile Giving Foundation Canada at support@mobilegiving.ca.

Chat: End users interact with a customer service agent or chat bot. Typically, a 1MO:1MT message ratio and conversational in nature.

Contests: Program offering a chance to win a prize.

Debt collection: Used to settle outstanding debts or delinquent accounts either directly by the creditor or on behalf of the creditor. Purchased debt collection (debt that has been sold from the original creditor) is considered a special use case.

Delivery notifications: Updates end users regarding the delivery status of an item.

Demo/testing: Used for demonstrations and/or for internal end-to-end testing purposes.

Fraud alerts: Used to flag suspected fraudulent activity or data breaches tied to an account.

Info-on-demand: Used to provide end users with one-time information such as product or service information.

Marketing: Notifying customers about sales and promotions to drive traffic to a website or a storefront.

Payment reminders: Used to remind end users of upcoming payments that are due or to remind of a missed or late payment.

Shared (common use only): Allows for multiple organizations or brands to share a single Common Short Code when the use case is common across all. Often also involves a common platform provider (e.g., for critical communications or surveys).

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

Transit updates or alerts: Used to send end users updates about a transit schedule (such as next bus or train arrival) or to provide updates about an upcoming flight.

Voting/surveys: Used to collect feedback or responses from an audience or customer. This can be done directly through the A2P channel or the A2P channel can be used to send a link to complete a survey or poll.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

Appendix C: Messaging protocols

	Short messaging service (SMS)	Multimedia messaging service (MMS)	Rich communication service (RCS)
Description	A communication standard for mobile messaging systems that enables sending text-based messages between mobile devices.	A communication standard for mobile messaging systems that enables sending multimedia messages (such as images and video files) between mobile devices.	A communication standard for compatible Android devices that enables sending messages between mobile devices using rich and enhanced features such as delivery and read receipts.
Benefit	SMS is ubiquitous: there are 34.6 million mobile subscribers in Canada[7] (approx. 88% of Canadians) and SMS is a standard feature on mobile devices.	MMS offers the ability to engage with an individual or group using images, audio, and video files, and can support significantly more characters in a single message.	RCS offers enhanced features such the ability to send larger, high-quality images, audio, and video streaming, as well as better group chat capabilities.

[7] https://canadatelecoms.ca/industry_data/mobile-phone-subscriptions/

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

Appendix D: A2P messaging channels

	Common Short Codes (CSC)	Toll-free numbers	10-digit long codes (10DLC)	Rich business messaging (RBM)
Description	A three- to six-digit number that replaces a traditional telephone number to send SMS or MMS messages to a mobile device	A 10-digit text-enabled toll-free phone number used to send SMS or MMS messages to a mobile device	A 10-digit text-enabled landline phone number used to send SMS or MMS messages to a mobile device	Communication channel between wireless carriers and compatible Android devices that uses data or Wi-Fi to provide enhanced messaging between businesses and end users
Oversight and regulation	Administered and monitored by the Association To view the most current version of the Canadian Common Short Code Application Guidelines, visit: https://www.txtca/en/apply-for-a-short-code/	Administered and monitored by Zipwhip	Self-regulated Expected to follow the same guidelines and best practices as CSC and toll-free numbers	Administered and monitored by Google
P2P/A2P	A2P	A2P	P2P	A2P
Protocol	SMS, MMS*	SMS, MMS*	SMS, MMS	RCS
Voice	No	Yes	Yes	Yes, in-app (tap to call)
Delivery reporting and receipts	Yes	Yes	No	Yes (includes read receipts)
Available price points (charged to end user)	Standard and free	Standard	Standard	Data/Wi-Fi-based

** Variable across wireless carriers*

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca

Appendix E: Regulatory resources

Businesses and organizations that leverage or support A2P messaging should be compliant with all current applicable rules that govern A2P programs in the Canadian and local markets through which the message is knowingly being delivered. Examples include:

Canada's Anti-Spam Legislation (CASL): An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the *Canadian Radio-television and Telecommunications Commission Act*, the *Competition Act*, the *Personal Information Protection and Electronic Documents Act* and the *Telecommunications Act*. For more information, visit: https://fightspam.gc.ca/.

***Digital Charter Implementation Act*:** Canadians increasingly rely on digital technology to connect with loved ones, to work and to innovate. That's why the Government of Canada is committed to making sure Canadians can benefit from the latest technologies, knowing that their personal information is safe and secure and that companies are acting responsibly. For more information, visit: Digital Charter Implementation Act, 2022.

Office of the Privacy Commissioner (OPC): An independent Crown entity that is funded by the state but is independent of Government or Ministerial control. For more information, visit: https://www.priv.gc.ca.

***Personal Information Protection and Electronic Documents Act* (PIPEDA):** This Act applies to private-sector organizations across Canada that collect, use, or disclose personal information in the course of a commercial activity. Organizations covered by PIPEDA should generally obtain an individual's consent before collecting, using, or disclosing that individual's personal information. For more information, visit: https://priv.gc.ca/.

Régie des alcools, des courses et des jeux: In Quebec, this government agency guides customers and informs them of their rights and obligations in the sectors of activity of alcoholic beverages, games, professional combat sports, and horse racing. It also supervises and monitors the activities of these sectors to ensure they take place in a safe, honest, and fair manner. For more information, visit: https://www.racj.gouv.qc.ca/.

Canadian Radio-television and Telecommunication Commission (CRTC): An administrative tribunal that Implements laws and regulations about Canada's communications systems and services. It regulates and supervises broadcasting and telecommunications in the public interest. For more information, visit: https://crtc.gc.ca/.

Competition Bureau of Canada: An independent law enforcement agency that protects and promotes competition for the benefit of Canadian consumers and businesses. Competition drives lower prices and innovation while fueling economic growth. For more information, visit: https://www.competitionbureau.gc.ca/.

1100-180 rue Elgin Street Ottawa, ON K2P 2K3
613-233-4888 | shortcodes@canadatelecoms.ca | txt.ca