

SPAM TOOLKIT

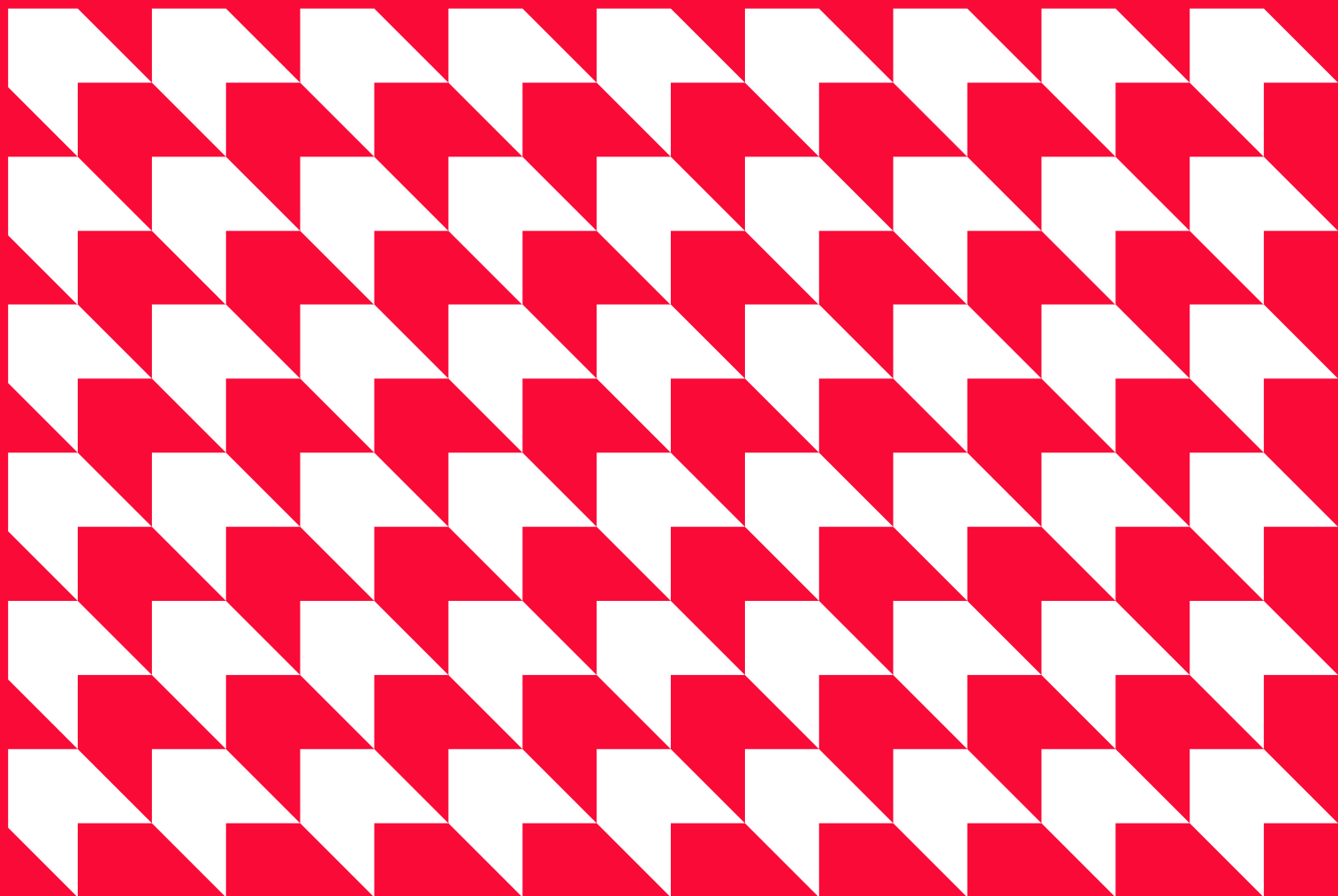
ADMA

Association for Data-Driven
Marketing and Advertising

DIRECT MARKETING AND LAWS AROUND SPAM

As updated August 2025

This document is intended to be used as an overview of current Spam regulations regarding commercial electronic messages. It is not intended to address the circumstances of any particular individual or entity nor is it to be used as a substitute for either legal advice or direct reference to Federal, State and/or Territory regulations.



DIRECT MARKETING AND LAWS AROUND SPAM

A direct marketer may communicate with an individual through a variety of channels, including via telephone, SMS, mail, email and online advertising. Direct marketing practices are primarily regulated through the *Spam Act 2003 (Cth)*, the *Do Not Call Register Act 2006* and the *Privacy Act 1998* (via APP 7).

In Australia, the sending of commercial electronic messages, via email, SMS, MMS, and/or instant messages, is governed by the spam laws.



A CLOSER LOOK AT THE SPAM LAWS OF AUSTRALIA

The Spam Act applies to “electronic messaging”, including messages sent via email, instant messaging, SMS and other mobile phone messaging, that have an “Australian link”.

DOES YOUR MESSAGE HAVE AN ‘AUSTRALIAN LINK’?

A commercial electronic message has an “Australian link” when one of the following conditions are met:

- › The message must originate in Australia;
- › The individual or organisation sending (or authorising the sending) of the message must be physically present in Australia (if an individual) or have its central management or control in Australia (in the case of an organisation); or
- › The messages must be accessible in Australia.

There are some exclusions, such as that commercial electronic messages may be sent by registered political parties or charities even if consent is not obtained. This is because in some instances these messages are not strictly considered to be ‘commercial’ or if it is, it falls within an exempt category. Note these exclusions are quite limited.

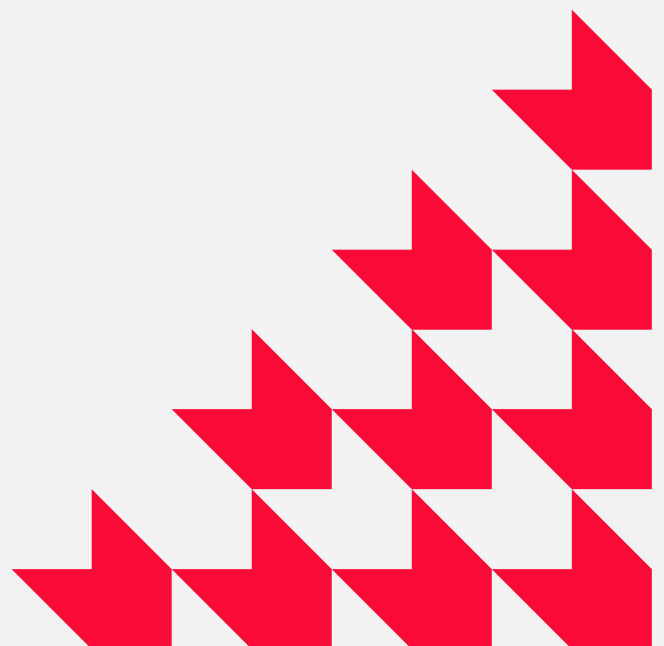
IS YOUR MESSAGE A COMMERCIAL ELECTRONIC MESSAGE?

To constitute a commercial electronic message, your message has to be both:

1. An electronic message; and
2. For a commercial purpose.

WHAT IS AN ‘ELECTRONIC MESSAGE’?

Your message is an electronic message if it is sent by SMS, MMS or to an email account, instant messaging account, telephone account or any other similar account.



IS THE MESSAGE FOR A 'COMMERCIAL PURPOSE'?

Under the Spam Act your message has a commercial purpose if it:

- > Offers, promotes or advertises goods and services, land or an interest in land, a business opportunity or investment opportunity.
- > Promotes or advertises a supplier of a good or service, land or an interest in land, a business opportunity or investment opportunity.
- > Assists or enables a person to (by a deception) dishonestly obtain property belonging to another person.
- > Assists or enables a person to (by a deception) dishonestly obtain a financial advantage or other gain from another person.

Other categories of messages

Two other categories of messages are relevant to understanding spam laws in Australia:

Transactional (or service) content messages:

These are messages where the primary purpose is transactional or service (or relationship) in nature, where the message only contains content that:

Facilitates or confirms a commercial transaction that the recipient already has agreed to;

1. Gives warranty, recall, safety, or security information about a product or service;
2. Gives information about a change in terms or features or account balance information regarding a membership, subscription, account, loan, or other ongoing commercial relationship;
3. Provides information about an employment relationship or employee benefits; or
4. Delivers goods or services as part of a transaction that the recipient already has agreed to.

Mixed content messages:

These are messages where both commercial and transactional content sit within the same message.

It is common for messages sent by businesses to mix commercial content and transactional or relationship content.

Importantly, even where commerciality may be the secondary purpose for the mixed message, the message is bound by the provisions of the Spam Act if it also contains commercial content. For example, a message that is mainly factual or useful information, but also includes some form of marketing or promotional content, would need to comply with the requirements of the Spam Act.

Note: If your message is not regulated under the Spam Act (i.e. it is NOT an email, SMS, MMA or instant message), it may still need to comply with regulations outlined in the [Do Not Call Register Act 2006](#) and / or Part 13 of the [Telecommunications Act 1997](#) (Cth).

REQUIREMENTS FOR SENDING COMMERCIAL ELECTRONIC MESSAGES:

Prior to sending a commercial electronic message, you must satisfy the following three requirements:



1. Obtain consent



2. Identify the sender (information about the sender)



3. Include an unsubscribe facility

1 Obtain consent

Prior to sending the commercial electronic message, you need to have consent from the individual or organisation (recipient). The Spam Act outlines two forms of consent: **express** and **inferred**.

Express consent is when an individual or organisation has deliberately and intentionally provided their consent by directly agreeing to receive commercial electronic messages from the sender. This can be done in a number of ways, such as the recipient filling out a form or ticking a subscribe checkbox on a website – as long as the recipient is aware of what they are consenting to.

Some examples include:

- › Ticking the box next to a statement seeking permission to send marketing messages;
- › Entering an email address on a competition entry form and ticking a box next to a statement that says they wish to receive regular updates on the activities of the business;
- › Contacting a business directly, in writing or over the phone, to ask for information to be sent to them on an ongoing basis.

You must keep a record when a person gives express consent, including who gave the consent, when and how. Under the Spam Act, it's up to you to prove that you have a person's consent.

Pre-checked tick boxes DO NOT count as consent. Consent to receive commercial electronic messages must be given actively and deliberately.

Inferred Consent relies on a relationship the message sender has with the recipient. An example is where the recipient has actively and knowingly provided their contact address, and it is reasonable in the circumstances to believe that they would expect to receive electronic marketing from your business.

A typical scenario where consent can be inferred is when the recipient is an existing customer of the relevant organisation and the message is related to a product or service that the customer has purchased from the organisation.

Consent may also be inferred in the following (limited) circumstances:

- › A person has made their email address or phone number public; and
- › that person does not state that they do not wish to receive commercial messages; or
- › The public email address or phone number is for an individual or office holder;
- › The message relates directly to the person's role or function and there is a link between the recipient and the content of the commercial message.

If you are not confident that consent can be inferred, you must obtain express consent.

If you are responding to a customer's enquiry, you have their consent to send them a commercial electronic message that is related to their enquiry only.

Can I use a purchased contact list?

Yes – however you need to ensure that consent has been obtained.

Organisations should be very careful when purchasing customer lists for the purpose of sending commercial electronic messages.

When sending commercial electronic messages using purchased lists, there is a risk that the business will not comply with the consent requirements of the Spam Act.

In addition, the Spam Act prohibits the use or supply of “address-harvesting software”. This is software that is used for, or marketed as being used for, searching the internet and collecting or otherwise harvesting, electronic addresses. The Spam Act further prohibits the use or supply of harvested-address lists, being lists created with address-harvesting software.

2 Identify the sender (information about the sender)

The message must contain clear and accurate information about the organisation who authorised the sending of the message. You must include information about how to contact your organisation. This information must be reasonably likely to be valid for at least 30 days after the message is sent.

Use the correct legal name of your business, or your name and Australian Business Number (ABN) in the message.

Understanding ‘identifying information’

Identifying information about the message sender may be found in:

- > The ‘from’ field or subject line of an email;
- > The body of the message text;
- > A website address and/or
- > The sender identification of an SMS or MMS message.

How to identify yourself when sending text messages

- > Using an alphanumeric sender ID (i.e. a word) on a text message may meet the requirement to identify the sender, however these types of sender IDs generally cannot receive return contact, and so would likely not, on their own, meet the requirement to include contact information.
- > Conversely, an SMS with a phone number as the sender ID would likely meet the contact information requirement, if the number can receive return contact and is monitored. However, it may not clearly identify the sender.

Remember that both obligations - (i) to clearly and accurately identify the sender and (ii) to include accurate information about how to contact the sender - must be complied with, when sending commercial electronic messages via SMSs.

3 Include an unsubscribe facility

All commercial electronic messages must contain a functional unsubscribe facility.

A message recipient must be given the option to unsubscribe, or withdraw their consent, to receiving commercial electronic messages. The commercial electronic message must include a clearly set out statement to the effect that the recipient may use the unsubscribe facility to send an unsubscribe message back to the sender.

For example:

- > **Email:** ‘If you no longer want to receive these messages, please click the following button to unsubscribe.’
- > **SMS:** ‘To unsubscribe, reply STOP’

Unsubscribe requests must be honoured **within five business days**.

It is good practice to deal with these as soon as possible to avoid being in breach.

SPAM REGULATIONS 2021

The Spam Regulations set out some further rules that your commercial electronic message must comply with, regarding an unsubscribe message:

1. The message must not require the recipient to use a premium service;
2. The message must not cost more than the usual cost of using that type of electronic address;
3. The message must not require the recipient to pay a fee/charge to the sender; and
4. The message must not require the recipient to:
 - › Provide personal information other than the recipient's address to which the message was sent
 - › Log into or create an account with the sender/organisation

A message does not have to be sent out to numerous addresses, or in bulk, to breach the Spam Act.

Businesses can also be responsible for breaches of the Spam Act by third-party contractors. If a business engages a third party to send a commercial electronic message/campaign on its behalf, the business needs to be aware of its legal obligations, as it may be found responsible for any contraventions of the Spam Act by the third party.

THE ACMA

The Australian Communications Media Authority (the ACMA) is responsible for administering and enforcing the following legislative instruments:

- › [The Spam Act 2003](#) (Cth) ('Spam Act') and the [Spam Regulations 2021](#) ('Spam Regulations') which regulates commercial electronic messages and prohibits the sending of unsolicited commercial electronic messages;
- › The [Do Not Call Register Act 2006](#) (Cth) which regulates unsolicited commercial calling to telephone numbers listed on the national Do Not Call Register; and
- › Part 13 of the [Telecommunications Act 1997](#) (Cth) which imposes restrictions on the use and disclosure of telecommunications and communications-related data.

The ACMA also investigates complaints, reports and enquiries about the above mentioned areas, and takes action when rules aren't being followed.

Investigations by the ACMA

Where the ACMA finds an organisation to be in breach of the law they can take the following actions:

- › Take the matter to the Federal Court, which can impose significant penalties;
- › Give the organisation an infringement notice;
- › Issue a formal warning;
- › Accept a court-enforceable undertaking

SUMMARY

Prior to sending a commercial electronic message, consider the following:

1

Is your message a commercial electronic message? If it is, you need to comply with the Spam Act rules.

2

Have you obtained consent from the recipient (either express or inferred)?

3

Does your message contain accurate information about you as the sender and does it contain your contact details (the sender)?

4

Does your message contain a functioning unsubscribe feature? You must then ensure that:

- › The recipient will not have to pay a fee to you (the sender); and
- › That the recipient is not required to provide personal information or log into/create an account with you (the sender).

FOR MORE INFORMATION:

[Australian Communications and Media Authority Website](#)

ADMA REGULATORY COURSES

1 DATA PASS COURSE

PROTECT YOUR REPUTATION BY PROTECTING YOUR CUSTOMERS' PRIVACY

Customers buy from brands and companies who respect their privacy. Earning and displaying the ADMA Data Pass Trustmark demonstrates that your company is qualified to handle data securely and appropriately. Human error is a leading cause of data breach. Data Pass is the best way to ensure your staff understand and comply with the laws that govern handling of personal information, reducing your data risk.

What is Data Pass?

The ADMA Data Pass is a comprehensive series of online training modules which focus on the areas of privacy and compliance in the collection, analysis and use of data in marketing and advertising. The ADMA Data Pass program is an exclusive program for ADMA members only.

[Get started](#)

2 SPAM LAW AND ELECTRONIC COMMUNICATIONS COURSE

The ADMA Spam Law and Electronic Communications short online course covers Spam and the rules governing the sending of commercial electronic messages.

It starts by outlining where the rules come from and the key piece of legislation that establishes the rules. It then considers the relationship with privacy law, before exploring how the rules apply in practice.

Finally, the course looks at how the rules are enforced by the regulator and presents case studies illustrating the consequences businesses may face for breaching those rules.

Enrol in this ADMA regulatory short course to gain a clear understanding of the rules that apply under the Spam Act 2004 and the Privacy Act 1988 – and their impact on the way businesses operate.

[Get started](#)

3 PRIVACY AND COMPLIANCE COURSE

NAVIGATE DATA PRIVACY LAW LIKE A PRO

Manage your marketing within the boundaries of privacy and compliance and get up to speed with current data privacy legislation.

Connecting with your customer in the digital age can be tricky. In an online world it's easier than ever, but just because you can doesn't mean you should. Don't risk your brand's reputation by breaking the law.

Duration: Two consecutive half days in our virtual classroom. Live and instructor-led interactive sessions.

[Get started](#)