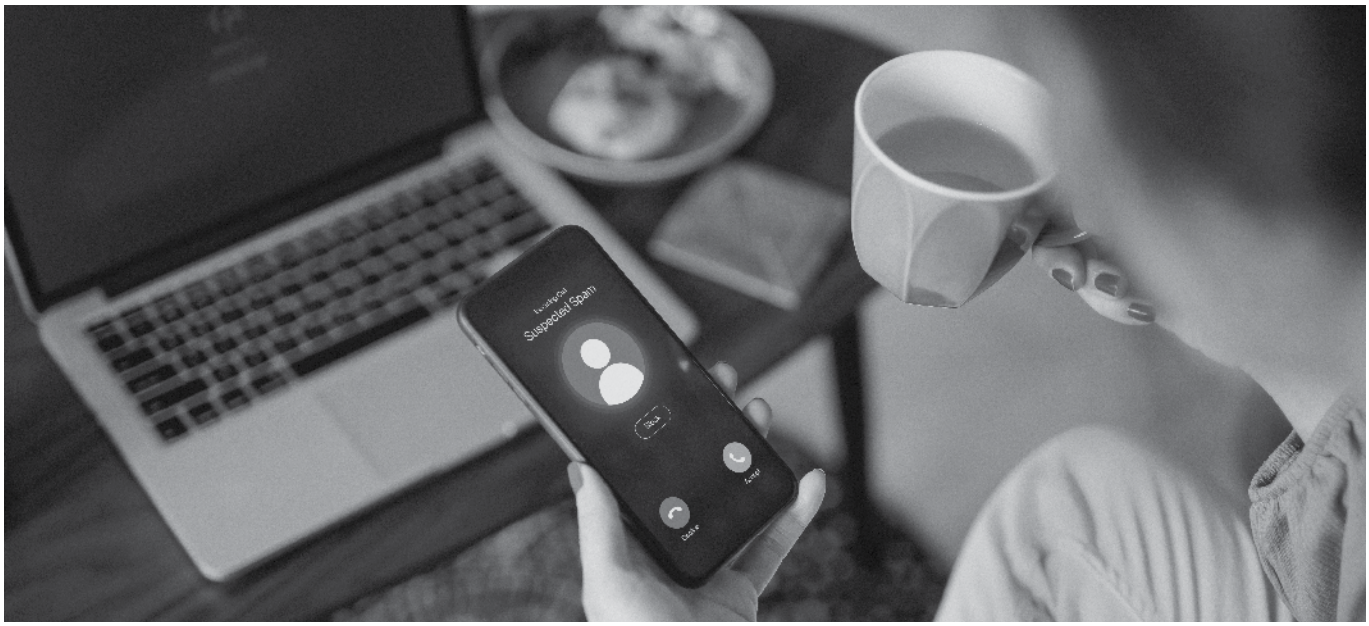

Understanding Spam Act obligations in financial services

Lynda Dowling

The *Spam Act 2003* (Spam Act) applies to most Australian businesses, including financial services, that send commercial messages for marketing or other purposes.

As such, the Spam Act sets out key requirements on how businesses can use mediums such as email, messages, telephone calls, SMSs and push notifications to contact other businesses and individuals.

The Australian Communication and Media Authority (ACMA) regulates the Spam Act. Further, unlawful financial services marketing has been a key compliance priority for ACMA.

On that, and upon the author asking industry peers at that time, it appears that ACMA is *not commonly known* by many financial services firms. As such, it is relatively easy to unwittingly/accidentally fall foul of this relatively unknown regulator in financial services. Upon the author asking industry peers at the time, they had not heard of ACMA.

This paper examines:

- key elements of the Spam Act
- ACMA's powers regarding financial services
- actions and items that are deemed breaches of the Spam Act, potential penalties and other costs.

ACMA's regulatory reach

As mentioned, ACMA is an independent Commonwealth statutory authority that regulates communications and media services in Australia.

ACMA:

- sets and manages rules about communications and media services (including in the context of financial services)
- licenses people, organisations and products to operate in Australia
- investigates complaints and problems, and takes action when its rules are not followed
- plans and manages the airwaves and makes space for new services like 5G.

As the regulator, ACMA can investigate matters covered by the:

- *Broadcasting Services Act 1992*
- *Radiocommunications Act 1992*
- *Telecommunications Act 1997*
- *Spam Act 2003*
- *Do Not Call Register Act 2006*
- *Interactive Gambling Act 2001.*

ACMA's powers regarding financial services

Whereas the Spam Act applies to most Australian businesses, it is believed the financial services industry has only recently fallen under

ACMA's remit as opposed to the broadcasting and media categories.

It is important to be mindful that it appears that ACMA was provided with additional funding from the federal government in 2022/23 to monitor the Spam Act further to include focusing on the financial services industry.

If ACMA finds a financial services firm has purposely or inadvertently breached the Spam Act *even just once*, during a very short period it can:

- provide a formal warning
- undertake a detailed investigation of the firm, with usually a large fine to follow
- commence civil proceedings against the firm through an Australian federal court of law, or
- impose an enforceable undertaking (EU) on the firm which involves appointing an independent expert, at a cost to the firm.

ACMA appears to work very differently from other regulators (such as the Australian Securities and Investments Commission (ASIC)). That is, if a firm inadvertently breached the Spam Act just once in a short period, an EU can be issued, whereas ASIC does not usually go down that path unless the matter was significant.

Implications for financial services firms

Breaches of the Spam Act are treated very seriously by ACMA. The challenges here for financial services firms (based on experience) are as follows:

- The overall fit of the financial services industry within ACMA's usual remit of media/communications/broadcasting, being:
  - it appears to be inexperienced in dealing with financial services firms, particularly those that are Australian financial services (AFS) licensees, Australian Prudential Regulation Authority (APRA)-regulated, and there may also be trading participants used to a different approach from other regulators
  - the Spam Act is in need of updating to bring it into line with the challenges of and approaches to today's technology
  - there appears to be a lack of alignment between ACMA and financial services regulations and guidance (e.g. ASIC's Regulatory Guide 234 *Advertising financial products and services (including credit): Good practice guidance*).
- The operational differences between ACMA and other regulators in that:
  - it *does not* appear to provide any additional guidance other than what is stipulated on its website (as opposed to detailed guides etc. on key regulatory requirements that other regulators issue in addition to information located on their websites)
  - based on the author's experience with ACMA, communication is minimal, with no warnings/formal warnings of a more serious manner of action it intends to undertake
  - as mentioned, there is no room for a second chance, based on evidencing key mitigants, upon breach of the Spam Act, unlike some financial services regulators who would do this
  - there appears to be no sliding scale of penalties (unlike those used by ASIC) whereby fines imposed by ACMA can be in the vicinity of millions of dollars.
- The length of the ACMA's EUs range from 12 to 36 months, thus:
  - causing financial services firms additional costs pertaining to appointing an independent expert, diverting resources to manage the EU, ensuring all relevant policies and procedures are in place, establishing frameworks for a detailed review, then dealing with the ongoing EU accordingly.

Working in conjunction with the Spam Act

Key polices that firms ideally should have in place to *act in conjunction* with the Spam Act are:

- a spam policy
- marketing policies and operating procedures
- a privacy policy.

Additionally, firms should have stringent marketing compliance controls within the firm's compliance and risk frameworks, and evidence monitoring of this.

Commercial electronic messages: Compliance essentials

Under section 6 of the Spam Act, a "commercial electronic message" (CEM) is defined as an electronic message that is *commercial* having regard to the content, the way in which the message is presented and the context of the message.

As an illustration, the following messages would be deemed to be CEMs if "it would be concluded that the purpose, or one of the purposes … is":

- an offer to supply goods or services
- advertising and promoting goods and services
- an offer to provide a business or investment opportunity
- assisting or enabling a person to dishonestly obtain property belonging to another person
- assisting or enabling a person to dishonestly obtain a gain from another person.

A CEM is commercial if it is motivated by a commercial purpose. It is important to be mindful that CEMs may still be deemed commercial *even if the CEM itself does not have an obvious commercial purpose*.

For example, a link to a webpage (such as a landing page which is an account-opening page of a financial services firm) within a CEM may be considered to have a commercial purpose.

Consent (permission)

Section 16(1) of the Spam Act *prohibits* the sending of "unsolicited commercial electronic messages". It also

Lynda Dowling, Webull Securities

Lynda is chief compliance officer within the local Australian entity of global financial services firm Webull, and played a key role helping the firm start up from scratch in Australia. She has over 20 years' compliance experience supporting high-performance businesses in investment banking, stockbroking, domestic commercial banking, and inter-dealer broking. Lynda holds the Governance Risk and Compliance Institute senior accreditation of Certified Compliance and Risk Professional (CCRP).

The quote

ACMA appears to work very differently from other regulators such as ASIC.

prohibits the sending of CMEs without *first* obtaining consent from the intended recipient.

To comply with this section, firms must have appropriate consent from anyone to whom the firm plans to send a CEM. Firms *cannot* use a CEM to seek a person's consent, as that would be a deemed marketing message by ACMA.

There are two types of consent:

- ***Express consent***—a person who gives express consent knows and accepts they will receive marketing emails or other commercial messages from the firm.
- ***Inferred consent***—in some circumstances, firms can infer that they have consent to send marketing messages if the recipient has knowingly and directly given their address.

Gaining express consent

Persons can provide their express consent by either of the following means:

- Filling in a form (ideally with an electronic signature)
- Ticking a box on a website (ideally with an attestation button)
- Over the telephone (ideally on a recorded line)
- Face to face.

The basis for inferred consent

Inferred consent is *not* as reliable as gaining someone's express consent, however, in *some circumstances* firms can infer that they have consent to send marketing messages if the recipient has knowingly and directly given their address. This is usually when a person has a provable, ongoing relationship with the business, and marketing is directly related to that relationship.

Identification

In accordance with section 17(1)(b) of the Spam Act, a CEM must include accurate sender information. Section 17(1) also contains additional criteria with which firms must comply.

Unsubscribe facility

Section 18(1) of the Spam Act contains the requirement that all CEMs (except "designated commercial electronic messages") must contain a functional unsubscribe facility at all times. This item ideally should be contained within the firm's compliance and risk frameworks for monitoring purposes.

Note: Designated CEMs are messages sent by government bodies, political parties, charities and educational institutions, or which consist of no more than factual information.

All unsubscribe requests must be honoured within five business days of receiving the request. It is usually a good idea to inform clients of this, as they may think it is instantaneous or at least within 24 hours.

In addition, the following mandatory requirements apply in relation to the unsubscribe facility:

- *Clear* unsubscribe instructions must be provided
- Clients are *not* subject to a fee for unsubscribing
- The unsubscribe function *must not require* the client to create an additional login, or log into an account in order to unsubscribe
- The unsubscribe function is functional for *at least 30 days* after the CEM has been sent.

CEMs with Australian links

Section 17(1) of the Spam Act requires that a CEM with an Australian link is *not* to be sent unless:

a) the message clearly and accurately identifies the individual or organisation who authorised the sending of the message; and
b) the message includes accurate information about how the recipient can readily contact that individual or organisation; and
c) that information complies with the condition or conditions (if any) specified in the regulations; and
d) that information is reasonably likely to be valid for at least 30 days after the message is sent.

In addition to the aforementioned requirements, section 7 of the Spam Act stipulates that a CEM has an Australian link if, and only if:

- the message originates in Australia, or
- the individual or organisation that sent the message is physically present in Australia when the message is sent, or
- the organisation's central management is in Australia when the message is sent, or
- the computer or device used to send the message is located in Australia, or
- the electronic account holder is an individual located in Australia, or
- the organisation carries on business in Australia when the message is accessed.

What happens when the Spam Act is breached?

When a firm breaches the Spam Act and is identified by ACMA either by a complaint or another manner, ACMA will then issue a compliance breach notification to the firm in question which will contain questions pertaining to the matter, and the ACMA enquiry will begin.

Regardless of how serious or not the breach is, ACMA can take any of the following actions:

- A thorough investigation of the firm, usually resulting in a large fine.
- Commence civil proceedings against the firm and key executives through the Australian federal courts (civil proceedings in a court of law can result in heavy penalties or even a prison sentence).
- Invite to firm to accept an EU from ACMA whereby the firm must pay for all costs to appoint an independent expert to undertake relevant tasks set by ACMA in the firm's EU.

Activities deemed to be breaches of the Spam Act

Essentially, if a firm sends out marketing emails or other

commercial messages, the firm must comply with the Spam Act.

Key breaches of the Spam Act are:

- failing to gain consent to send such messages (consent can be either express or inferred)
- failing to identify yourself as the sender (using the correct legal name of your business, your name and Australian Business Number (ABN))
- failing to make it easy for persons to unsubscribe
- including unsubscribe language that is not clearly worded.

Other actions that may breach the Spam Act are:

- using or supplying a list created with address-harvesting software; or supplying the address-harvesting software
- helping, guiding or working with another person to breach the Spam Act
- encouraging another person to breach the Spam Act.

Case studies and associated penalties

Following is a summary of recent case studies pertaining to financial services along with the penalties imposed for breaching the Spam Act:

- *June 2023: Commonwealth Bank of Australia* was fined $3.5 million for issuing more than 61million marketing emails that unlawfully required the bank's customers to log in to unsubscribe. Additionally, the bank sent out a further 4 million marketing messages that failed to have a functioning unsubscribe facility. An EU was also imposed.
- *December 2022: Binance Australia* was fined just over $2 million and received a three-year EU for sending out 5.7 million commercial emails that made it difficult for consumers to opt-out by requiring them to log into an account. Further, Binance sent out 25 emails without the recipients' consent.
- *September 2022:* Latitude Financial was fined $1.55 million after ACMA found that Latitude had mischaracterised commercial emails and texts that were promoting the firm's products as "information only", thus being in breach of the Spam Act.
- *February 2022:* Phoenix Securities was fined $26,640 in addition to an EU being imposed after the firm sent over 3,000 emails without consent offering business loans.

Conclusion

To avoid any electronic communications falling into ACMA's classification of spam:

- ensure you understand how to comply with the Spam Act
- always gain consent
- identify yourself as the sender
- make it easy for clients to unsubscribe
- avoid undertaking other actions that may contravene the spam rules
- have marketing compliance frameworks in place (to include monitoring and testing)
- have key policies and procedures in place pertaining to the Spam Act
- ensure relevant employees are provided training in relation to the Spam Act and the firm's internal controls etc.

Remember, a firm only needs to *inadvertently* breach the Spam Act *once* during a *very short timeframe* for an EU to be imposed. **FS**

The quote

The Spam Act prohibits the sending of commercial electronic messages without first obtaining consent from the intended recipient.