

# Scams - Mandatory Industry Codes Consultation Paper

Jan 2024

Ref: <https://treasury.gov.au/consultation/c2023-464732>

There is no doubt that we need efficient and effective measures to counter scams. To that end, we support the motivation behind this paper to look for ways to prevent, detect and repair the damage caused by scams.

We believe the approach can be improved in two main areas:

- 1) Scope.** The “whole of ecosystem approach” proposed is true, but then narrowly constrained to just three types of industry participants. Why? Scammers will, as pointed out in the paper, exploit any and all weaknesses. This means that scammers will seek to exploit any and all government and business types where a financial outcome can be triggered (which basically means ALL government and business types).

Proposal: Broaden the scope to include all industries. We recognise that this might mean it needs to transfer to another government entity, perhaps the ACCC if we are seeking to protect consumers?
- 2) Focus.** Much of the approach proposed focuses on educating, protecting and identifying the individual. This is necessary, but not sufficient. Many scams attempt to defraud their victims by pretending to be an organisation (using SMS codes, look-a-like websites, fake letters, fake phone calls etc). While the paper makes reasonable efforts to propose ways in which **fake** communication might be identified, it makes no suggestions on how **legitimate** communication should be authenticated. While customers cannot identify fake organisation communications from real, they are vulnerable to fraud.

Proposal: Add a prevention principle along the lines of: “a business must seek to authenticate itself to its customers on every channel and in every communication.” While this may require a “reasonableness” approach depending on context and content, the principle should remain the same, and technology solutions exist for organisations to use on each channel.
- 3) Measure of success.** There is little/no attempt to provide evidence based links between the incidence of scams and these measures, either in the prevalence before enacting these measures, or in the hoped for impact of these measures. Without the ability to prove that the code has had a beneficial impact, there can be no certainty that it has worked, beyond providing a reassuring and announceable gesture.

John Phillips  
Co-Founder Sezoo

Jo Spencer  
Co-Founder Sezoo



# Specific Comments on Questions in Paper

Number	Sezoo Comments
Q1	We think improvements are possible. The scope should be widened to the whole of the Australian economy; the focus should include organisation’s authenticating themselves to their customers (and other organisations); and there should be a way to measure the impact of the Framework.
Q6	See answer to Q1
Q8-14	There seems to be a risk here of thinking that a “perfect” definition of a type of crime will better enable its prevention. It would be better if it were possible to avoid such minutiae. If something is against the law, it should be against the law irrespective of “how” it is achieved. Breaking into someone’s house should be illegal regardless of what tools you use. Deceiving someone into getting them to give you the keys to their house (so you can rob them) should be illegal regardless of the method of deceit used.
Q15, Q22, Q35	All businesses should declare their public commitment to the principles in the paper, including the additional principle we propose of authenticating themselves in their communications with their customers.
Q24	This question is somewhat concerning as it gives an impression that scams should be of the highest concern. Our perspective on this is “yes, but”. There are many (many) ills that can befall customers of organisations. Scams are but one. We would prefer that all organisations have a strategy that considers “how best might we protect our customers” of which an anti-scam approach is just ONE dimension.

