Submission

To	The Treasury Department
Topic	**Scams Prevention Framework codes and rules exposure draft**
Date	June 2026

Contact

E advocacy@unitingcommunities.org

P 08 8202 5111

UNITING COMMUNITIES

About

Uniting Communities is an inclusive not-for-profit organisation supporting more than 115,000 South Australians each year and has been creating positive change for communities for over 120 years. We advocate for systems change across diverse social justice issues to shape public and social policy that delivers better outcomes for marginalised communities.

Law Centre

Uniting Communities Law Centre provides free and independent legal help to people experiencing disadvantage across South Australia. We understand that dealing with the legal system can be confusing and daunting and staff in the Uniting Communities Law Centre assist people to work through these challenges. The qualified team provides support with information, advice, representation, referrals, or community legal education.

Consumer Credit Law Centre SA

The CCLCSA was established in 2014 to provide free legal advice, representation, legal education, advocacy and financial counselling to consumers in South Australia in the areas of credit, banking and finance, including circumstances involving scams. The CCLCSA is managed by Uniting Communities. Over the years, CCLCSA staff have advised and supported clients who have experienced significant scam losses, sometimes in the hundreds of thousands of dollars. The team has seen the devastating impact of those losses and welcomes all reform to improve protections for consumers.

Submission to Scams Prevention Framework codes and rules exposure draft

Uniting Communities thanks the Treasury Department for the opportunity to provide feedback on the Scams Prevention Framework codes and rules exposure draft. We recognise the significant work undertaken to reach this stage.

These proposed reforms address several longstanding issues associated with scams, including inadequate protections for many banking customers in relation to abnormal and suspicious transactions. Uniting Communities' services, particularly our Law Centre and the Consumer Credit Law Centre SA, regularly support clients experiencing financial hardship because of scams.

The prevalence of scams continues to increase, driven by the growing use of online technologies and an ageing population, leaving many individuals vulnerable to these crimes.

Uniting Communities broadly supports the proposed changes and enhanced consumer protections, including mandatory reimbursement and strengthened obligations on regulated entities. This submission outlines a number of recommendations, with a primary focus on the banking sector.

In particular, we have concerns regarding the practical implications of the proposed expectation of shared responsibility and collaboration between banks, digital platforms, and telecommunications providers. While we support the intent of this approach, there is a risk that, without formalised processes or mechanisms to facilitate coordination, this expectation may lead to unintended adverse outcomes for consumers. We also note that some entities appear to be excluded from the proposed framework, including platforms such as Facebook Marketplace, even where they operate as part of a larger digital platform (e.g. Meta).

Our key recommendations:

- **Provide clear guidance on completing Statements of Compliance to ensure mandatory information is consistently included, enabling consumers to make informed decisions about whether to escalate matters to AFCA.**
- **Establish a formal external mechanism to coordinate multi-party dispute resolution, and clarify the roles and responsibilities of each entity in relation to information sharing and liability.**
- **Monitor and respond to the risk of increased debanking among vulnerable customers as banks implement SPF obligations. Encourage the industry to develop products that allow higher-risk clients to retain access to essential banking services.**
- **Recognise the critical role of information-sharing provisions in determining the effectiveness of the framework, noting that the intelligence-sharing and reporting obligations will remain limited until there is clarity on what information can be shared and how.**

Consultation

Statement of compliance

We support the requirement for entities to issue statements of compliance in response to internal dispute resolution (IDR). Their effectiveness will depend on the level of detail provided. A standardised Statement of Compliance form and/or clear guidance would help ensure the information requirements under section 2.1 are consistently met, enabling consumers to make informed decisions about whether to escalate a matter to AFCA.

Sufficient supporting evidence is also critical in enabling consumers to assess whether to accept compensation. In the absence of this information, consumers may feel pressured to accept inadequate compensation outcomes. It is unclear whether the exclusion of information that is *commercially sensitive*, or *personal information (2-1 (3)*, would prohibit necessary information from being included in the statement of compliance.

Additionally, the requirement that the statement be *easy to understand including by a person with a disability, from a cultural or linguistically diverse background, or with other special needs*, will require additional guides and resources for entities to fulfill. Ideally, the requirements for making a statement easy to understand should be outlined specifically within the rules to avoid subjective decision making.

Further consideration should also be given to circumstances where incorrect or misleading information is provided (whether intentionally or inadvertently), and to the safeguards required to ensure accountability in such cases.

13. Does the draft code effectively require cooperation between entities during internal dispute resolution to support consumers making complaints involving more than one entity?

Multi-party dispute resolution

While the ability for consumers to lodge a complaint with more than one entity is a positive reform, in practice, meaningful collaboration between entities will be difficult to achieve without a formal external mechanism to facilitate coordination. Section *2-26 (1) (2) Cooperation between regulated entities*, places significant responsibility on the *first entity,* to facilitate information sharing and *apportion liability.* Without sufficient oversight this collaboration appears unrealistic in practice and risks entities taking a narrow approach to their responsibilities, particularly where obligations are ambiguous. This may result in complaints being redirected between entities, creating additional barriers for consumers seeking timely resolution.

It is our understanding that AFCA will only get involved after IDR, on the assumption that multiparty IDR will occur. While there are obligations for entities to cooperate the detail is light, with responsibility placed on entities to create their own systems to carry out this cooperation. In reality, because this system doesn't exist the onus will likely be on AFCA to facilitate coordination once consumers have escalated the matter. Additionally, while banks already operate within existing IDR obligations, digital platforms and telecommunications providers may not have comparable systems or infrastructure in place, potentially leading to inconsistent consumer outcomes in the interim.

17. Does the draft code include sufficient obligations on sending banks to disrupt scam activity (division 4), and is it clear that the disrupt obligations extend to both sending and receiving banks?

We recommend that provisions within the legislative instruments are drafted as clearly and precisely as possible. For example, while both sending and receiving banks are intended to be captured by the new obligations under section 3-3, some references to "customers" in the explanatory statement may inadvertently imply responsibility only for the sending institution. This ambiguity could be addressed through strengthened and more precise drafting.

Compensation

We wholeheartedly support reforms that enable timely compensation for consumer scam losses.

While the proposed automatic compensation model for losses under $3,000 would be a welcome step toward a simpler remediation experience for consumers, key details regarding its application, limits, and safeguards are currently lacking. Automatic compensation will be a positive development if it genuinely simplifies the complaints process. However, we are concerned about how it will operate in practice, particularly when considering the expectation of shared liability across regulated entities.

Key questions include:

- Will a single entity in the scam chain provide automatic compensation, or will consumers be required to engage with multiple entities?
- Will consumers who have experienced higher losses be eligible for automatic compensation for the first $3,000, with remaining losses subject to a full assessment of a regulated entity's compliance with the SPF?
- Is the $3,000 limit applied per scam instance?
- Does the limit apply per regulated entity, or is it attached to the consumer?
- Is it an annual limit, or a lifetime cap for each consumer?

In addition, the position paper refers to "verified" scam losses. While verification is understandable, and likely necessary as a safeguard against exploitation of the reimbursement process, it remains unclear what the verification process will involve from the consumer's perspective.

Clarification on these issues will be critical to determining whether the proposed automatic compensation model can deliver on its stated objectives: streamlining processes, supporting timely resolution, and minimising the cost of investigating complaints.

Debanking

There is a risk that debanking practices will increase as banks take on expanded obligations to proactively detect and respond to scams. This may lead to heightened identification of customers perceived as high risk. Vulnerable individuals, including those who are repeatedly targeted by scams or who lack the capacity to identify scam activity, may face an increased risk of having their access to banking services withdrawn. Banks may be more inclined to de-risk by closing accounts where customers are seen as a potential liability.

Debanking can have significant downstream impacts, including reduced access to essential services such as housing and social security payments. There is also a risk that individuals may be debanked where they are unaware their accounts are being misused by scammers, leading to potential mischaracterisation as perpetrators.

While the proposed rules contain some provisions relating to debanking (e.g. identification in section 3-3 & 3-12 (1) (b)), more protections are needed because of banks' discretion to withdraw services. We recommend further consideration of protections for affected customers, including:

- clear and accessible remedy pathways following debanking decisions (including further provisions under 3-12 (1) (b) and
- the development of restricted or safeguarded banking products for high-risk customers, which maintain a level of financial autonomy while mitigating exposure to scams.

Conclusion

We appreciate the opportunity to provide a submission on the Scams Prevention Framework codes and rules exposure draft. Uniting Communities is broadly supportive of the proposed changes, that will strengthen both the proactive action and response to Scams in Australia. The additional changes proposed in our submission will further strengthen the legislative instruments and support effective implementation.

Case studies (de-identified)

Melissa*, a 55-year-old woman who retired early from the workforce on medical grounds, saw a Facebook advertisement promoting a cryptocurrency training program and the potential to make money from it. She was interested in learning more and, having time on her hands, provided her details. She later began speaking on the phone with Andrew, a trainer for the company.

Melissa and Andrew spoke frequently, and he eventually convinced her to begin investing in cryptocurrency. She was coached on how to withdraw all of her superannuation and later open multiple cryptocurrency trading accounts, transferring all of her money into those accounts and then "investing" it in crypto (by making transfers to the scammers).

Melissa lost over $500,000 and was unsuccessful in her scam complaint against the bank, which did not intervene when she began making sudden, significant transfers to cryptocurrency exchanges.

In a post-SPF environment, we would expect that the bank, in carrying out its prevent, detect, and disrupt obligations, would have intervened to stop these transfers and could have saved Melissa's retirement savings from being stolen.

*name changed for privacy