info@consumeraction.org.au
consumeraction.org.au
T 03 9670 5088
F 03 9629 6898

25 August 2026

ENSURING THE SCAMS PREVENTION FRAMEWORK WORKS FOR FIRST NATIONS CONSUMERS

Consumer Action Law Centre and Mob Strong Debt Help joint supplementary submission

This supplementary submission is made on behalf of Consumer Action Law Centre and Mob Strong Debt Help. It should be read alongside our main joint consumer submission on the Scams Prevention Framework (SPF), submitted on Friday 3 July 2026. This submission considers whether the SPF will provide effective, accessible and culturally safe protections for First Nations consumers and highlights the distinct barriers First Nations consumers may face in responding to scams. These barriers include remoteness, digital exclusion, limited access to business branches and culturally inappropriate financial, telco and digital platform systems and complaint processes.

It recommends targeted changes to ensure the SPF does not reproduce existing inequalities and that regulated entities are required to design their systems, support and dispute resolution pathways with and for First Nations consumers and communities.

A summary of recommendations is available at **Appendix A**.

Use of Artificial Intelligence

Artificial intelligence (AI) tools were used to assist with administrative and editorial tasks in the preparation of this submission, including formatting, document organisation, proofreading and language refinement. The analysis, recommendations, legal and policy positions, and substantive content of the submission were developed, reviewed and approved by Consumer Action Law Centre staff.

TABLE OF CONTENTS

About Consumer Action Law Centre

Consumer Action Law Centre is an independent, not-for profit consumer organisation with deep expertise in consumer and consumer credit laws, policy and direct knowledge of people's experience of modern markets. We work for a just marketplace, where people have power and business plays fair. We make life easier for people experiencing vulnerability and disadvantage in Australia, through financial counselling, legal advice, legal representation, policy work and campaigns. Based in Melbourne, our direct services assist Victorians and our advocacy supports a just marketplace for all Australians.

Overview

The SPF must recognise that First Nations consumers can experience scam harm differently because of geographical, digital, financial, cultural and service-access barriers. These differences do not arise from any inherent vulnerability of First Nations people. They instead reflect structural exclusion, the design of mainstream financial and digital systems and the failure of many service providers to deliver culturally safe and accessible support.

Evidence points to disproportionate harm. In the first half of 2025, Scamwatch recorded a 55.3 per cent increase in reports involving financial loss from First Nations consumers compared with the same period in 2024.[1] Scamwatch data from 2021 recorded 4,958 reports and $4.8 million in losses from First Nations peoples, representing a 142 per cent increase in reported losses from 2020.[2] However, the reported figures are likely to understate the scale of harm because many consumers may not be able to report scams or reach external dispute resolution.[3]

Recent data also shows that some scam types disproportionately affect First Nations communities. For example, Scamwatch data indicates that more than 45 per cent of reported losses to "scambling" in 2025 came from consumers who self-identified as First Nations.[4] This reinforces the need for the SPF to support targeted, community-led responses as scam methods evolve.

The SPF codes should include specific, enforceable obligations to ensure bank, telecommunications providers and digital platforms consider the circumstances of First Nations consumers when preventing scams and providing assistance after scam harm occurs.

First Nations consumers face heightened scam risks

First Nations consumers can face increased vulnerability to scams due to a range of structural, historical and systemic factors that influence access to information, services and protections. These factors should be recognised in the design and implementation of the SPF.

Key factors include:

- The ongoing impacts of colonialisation, which disrupted traditional economic systems and contributed to the exclusion of many First Nations people from mainstream financial services.
- Historical government control over the financial affairs of First Nations peoples and limited opportunities for economic participation have affected the development of financial capability across generations.
- A documented history of exploitative sales practices targeting First Nations communities. In some cases, vulnerable consumers have been recruited to promote products or schemes within their own communities, leveraging existing relationships and trust. The Federal Court's decision in *ACCC v Cornerstone Investments Pty Ltd (In Liq)(No 4)* illustrates how unconscionable conduct can occur in these contexts.
- Cultural communication dynamics, including the phenomenon of gratuitous concurrence, where a person may agree with a proposition or representation from an authority figure or dominant source, despite not fully understanding the information presented or having had a genuine opportunity to consider it (for example, a representation made on a social media advertisement).
- First Nations peoples are more likely to experience a digital gap in their communities, are less able to access advocacy services and kinship in communities can increase the fear of shame to disclose their loss.

---

[1] National Anti-Scam Centre calls for continued action this Scams Awareness Week as scam losses trend up at $174M | ACCC.
[2] Scam losses to culturally diverse communities, people with disability and Indigenous Australians almost doubled in 2021 | Scamwatch.
[3] AFCA complaints reveal ongoing barriers for Aboriginal and Torres Strait Islander consumers | Australian Financial Complaints Authority (AFCA).
[4] New taskforce to tackle 'scambling' as fake online casinos target First Nations Australians | ACCC.

The SPF should recognise these factors and adopt a culturally informed approach that addresses both immediate scam harms and the underlying conditions that can increase susceptibility to scams.

"Scambling" in First Nations communities

Scambling is a growing issue where consumers are drawn into illicit online gambling or gaming platforms through social media advertising, direct messages or other channels.

Consumers are typically enticed with promises of significant financial returns. Consumers deposit funds into the platform and may be shown apparent winnings but are ultimately unable to withdraw their money. In some cases, consumers have also provided banking or account details that are then misused by criminal actors, including for suspected money laundering activities.

Some major banks have started measures to contact and engage with customers or communities when suspicious activity is detected to provide scam warnings and education. However, some consumers report being warned that continued engagement with these platforms could result in debanking if they continue with scambling. There is a risk that some customers are not able to understand the warning, let alone receive it, and subsequently find out they have been debanked without knowing why.

This response can cause significant adverse consequences for First Nations consumers, particularly in regional and remote communities where banking options are limited. Debanking can reduce access to financial services, increase financial exclusion and exacerbate existing barriers to participation in the digital economy. Scam prevention measure must therefore prioritise consumer protection, education and support without creating disproportionate harms for people who are themselves victims of scams.

RECOMMENDATION 1. Regulators should assess whether regulated entities are effectively enabling First Nations consumers to report scams, seek assistance and obtain remedies. Audits and compliance activities should include consideration of accessibility, cultural safety and measures to minimise the evidentiary burden on scam victims.

RECOMMENDATION 2. Regulated entities should ensure data collection, management and sharing practices are consistent with First Nations Data Sovereignty principles, including mechanisms that enable First Nations peoples to access and exercise greater control over data relating to them and their communities.

RECOMMENDATION 3. The SPF should consider its interaction with current and future reviews and reforms relating to lead generation, unsolicited selling and digital advertising practices, as these practices can facilitate the targeting of First Nations consumers by scammers.

Digital exclusion creates barriers to scam prevention and support

First Nations consumers are not a homogenous group. Experiences vary between urban, regional, remote and very remote communities and are affected by factors including income, disability, age, language, education, housing and access to services.

Digital exclusion is a significant concern. First Nations consumers are twice as likely as other consumers to experience digital exclusion, while three in four First Nations people living in remote and very remote communities are digitally excluded.[5] Limited connectivity, device access, affordability and digital support can restrict people's ability to receive scam warnings, access online banking, report scams, secure compromised accounts or participate in digital complaint processes.

[5] New Report: First Nations Australians twice as likely to be digitally excluded - Australian Digital Inclusion Index.

These barriers are particularly important because banking, telecommunications, government and complaint services increasingly operate online. A consumer experiencing unreliable mobile coverage may be unable to contact their bank quickly, receive authentication messages, report a scam or respond to a fraud alert. Automated systems may also overlook language barriers, digital exclusion, financial hardship, disability or financial abuse. The Australian Financial Complaints Authority (AFCA) has warned that branch closures, unreliable connectivity and limited cultural understanding continue to create barriers for First Nations consumers, particularly in regional and remote communities.[6]

RECOMMENDATION 4. Require regulated entities to co-design accessible and culturally safe scam reporting and support channels with First Nations communities, including non-digital options, interpreter services and trusted representative arrangements.

RECOMMENDATION 5. Government, together with industry, should fund First Nations financial counsellors, legal services and Aboriginal Community-Controlled Organisations (ACCO) to provide rapid, culturally safe assistance to scam victims.

Branch closures and inaccessible scam-response systems

The loss of bank branches and face-to-face services can have serious consequences in a scam context. A consumer in a remote community may need to travel significant distances to verify their identity, restore access to an account or speak to someone about suspicious activity. Cases reported through remote banking programs include consumers travelling several hours to complete identity checks, being unable to access accounts after failing standard identification questions and being unable to adjust account security settings.[7]

While speed is critical when responding to scams, the SPF currently assumes that all consumers can readily access digital or telephone support. That assumption will not hold for consumers who have limited connectivity, limited access to devices or no nearby branch. A requirement to provide a 24-hour reporting mechanism as per section 2-18(1)(d) of the common SPF code provisions will not work in practice for First Nations consumers if the mechanism is automated, difficult to navigate, dependant on reliable connectivity or unable to accommodate language and accessibility needs.

RECOMMENDATION 6. The codes should require regulated entities to maintain culturally safe and accessible alternatives to digital self-service. This should include dedicated First Nations customer support, access to trained staff, interpreter services, assisted complaint pathways and arrangements for face-to-face or community-based support where digital engagement is not readily available. Having these services will give a practical reason for requesting a customer's First Nations status for better reporting and will be in satisfaction of Australian Privacy Principle 3.[8]

Cultural practices must not be treated automatically as consumer misconduct

The SPF must also recognise that mainstream banking assumptions may not reflect the ways resources are shared within some First Nations families and communities. Cultural and kinship obligations can involve collective approaches to money, reciprocal support and sharing resources across extended family or community networks.[9] First Nations-led research has highlighted the need for institutions to understand these social and economic systems and to distinguish legitimate cultural sharing from coercion, exploitation and financial abuse.[10]

---

[6] AFCA complaints reveal ongoing barriers for Aboriginal and Torres Strait Islander consumers | Australian Financial Complaints Authority (AFCA).
[7] The program helping remote First Nations Australians access banking.
[8] Chapter 3: APP 3 Collection of solicited personal information | OAIC.
[9] ASIC's Indigenous Financial Services Framework.
[10] A path forward for First Nations people experiencing financial abuse.

Practices such as sharing a bank card, PIN, device or account access may occur in some circumstances because a trusted family or community member assists with shopping, banking, language, transport or navigating digital services. These practices can create security risks, but they should not automatically be characterised as negligence, fraud or a reason to deny remedy and compensation. Australia's financial system is largely designed around individual account control and may struggle to accommodate trusted assistance and collective approaches to resource sharing.

RECOMMENDATION 7. Banks should be required to investigate the full cultural and practical context before relying on card, PIN or credential sharing to reject a claim. They should also explore with the customer and provide safer alternatives, such as culturally accessible account controls.

Financial and digital capability responses must be culturally safe

Lower levels of financial or digital capability should not be used to shift responsibility for scam prevention onto First Nations consumers. Financial capability is shaped by access to appropriate services, historical exclusion, education, income, language and whether information is provided in a culturally relevant form. ABA member banks explicitly recognise that First Nations consumers, including people in remote locations, can experience increased vulnerability and barriers to accessing banking services.[11]

Consumer awareness campaigns alone will not be sufficient. Scamwatch's First Nations resources and community-focused material are a useful starting point, but these initiatives should complement, not replace, strong prevention obligations on regulated entities.[12]

RECOMMENDATION 8. Scam warnings must be available in plain English and First Nations languages in accessible formats and should be developed together with First Nations organisations and communities. Information should also be delivered through trusted local channels such as ACCOs, Indigenous financial counsellors, local radio, community centres and face-to-face outreach.

Cultural capability must be embedded in SPF training

While section 2-3 of the common SPF code requires staff training, this provision should also explicitly require First Nations cultural capability and culturally safe scam responses. Generic vulnerability training is unlikely to equip staff to understand the effect of remoteness, kinship obligations, language differences, shared devices, limited identification documents, digital exclusion or distrust of mainstream institutions.

RECOMMENDATION 9. At a minimum, the SPF should require staff who make scam-prevention, account-restriction, complaint or compensation decisions to be trained to recognise structural and service-access barriers experienced by First Nations consumers, understand culturally specific approaches to sharing money and resources, communicate through interpreters and culturally safe channels, avoid blaming or shaming consumers, provide trauma-informed assistance and appropriate referrals, and work effectively with ACCOs, First Nations financial counsellors and trusted support people.

RECOMMENDATION 10. Training content should be developed and reviewed with First Nations-led organisations. Regulated entities should also be required to measure training effectiveness, rather than merely recording staff attendance.

[11] ABA Industry Statement: Supporting Aboriginal and Torres Strait Islander peoples.
[12] Resources for First Nations peoples | Scamwatch.

Culturally safe reporting and response pathways are essential

First Nations consumers may be less likely to report scams or pursue complaints where services are not culturally safe, trusted or accessible. Experiences in insurance and other financial services show that cultural and kinship practices can shape how consumers understand risk, share resources and seek support when something goes wrong. Strong community and family support are important and valid sources in the process and should be treated as such, but mainstream financial systems might not recognise these practices or clearly explain the role of institutional protections, complaint pathways and compensation.

These cultural and institutional factors can also shape how First Nations consumers report scams and seek redress. Feelings of shame, fear of judgement, limited understanding of available rights and previous negative experiences with institutions may discourage come consumers from reporting a scam or progressing a complaint. However, these issues should not be framed as shortcoming of First Nations consumers. They instead reflect whether reporting and dispute resolution systems are culturally safe, accessible and responsive. AFCA's own work recognises the importance of culturally competent complaint resolution and First Nations voices in the delivery of financial services.[13]

RECOMMENDATION 11. Under the SPF's respond pillar, regulated entities should be required to provide culturally safe reporting and complaint pathways, developed in collaboration with First Nations organisations and communities.

Identity verification requirements must not deepen exclusion

Stronger identity verification requirements under the SPF may assist in preventing fraud and scams, but they also risk creating further barriers for First Nations consumers who do not hold conventional forms of identification. This is particularly significant in remote communities where people may not have a birth certificate, driver's licence or other standard identification and may have different names or dates of birth recorded across government and service-provider systems.

The community identification card project, which is developing a framework for ACCOs to issue approved cards, provides a culturally appropriate alternative. Recognising these cards would allow the SPF to strengthen identity controls without excluding First Nations consumers from banking, telecommunications and other essential services.

These cards are issued by Aboriginal corporations, land councils, local governments and other community organisations. The cards vary in their level of sophistication and can contain identifying information such as the person's name, photograph, date of birth, address, signature and a unique reference number.[14] Those with greater sophistication will be more readily acceptable by banks.

The Australian Banking Association has developed guidance to help banks assess and accept these cards for Know Your Customer identification purposes, consistent with the Australian Transaction Reports and Analysis Centre (AUSTRAC) guidance encouraging a flexible approach for First Nations customers who do not have standard identification.[15]

RECOMMENDATION 12. The SPF codes should expressly recognise First Nations community identification cards as an acceptable form of identification and require banks and other regulated entities to offer alternative verification pathways in compliance with AUSTRAC's guidance for identification.

[13] AFCA Engagement with First Nations peoples | Australian Financial Complaints Authority (AFCA).
[14] ABA-First-Nations-Community-ID-Factsheet.pdf.
[15] Ibid.

APPENDIX A - SUMMARY OF RECOMMENDATIONS

RECOMMENDATION 1. Regulators should assess whether regulated entities are effectively enabling First Nations consumers to report scams, seek assistance and obtain remedies. Audits and compliance activities should include consideration of accessibility, cultural safety and measures to minimise the evidentiary burden on scam victims.

RECOMMENDATION 2. Regulated entities should ensure data collection, management and sharing practices are consistent with First Nations Data Sovereignty principles, including mechanisms that enable First Nations peoples to access and exercise greater control over data relating to them and their communities.

RECOMMENDATION 3. The SPF should consider its interaction with current and future reviews and reforms relating to lead generation, unsolicited selling and digital advertising practices, as these practices can facilitate the targeting of First Nations consumers by scammers.

RECOMMENDATION 4. Require regulated entities to co-design accessible and culturally safe scam reporting and support channels with First Nations communities, including non-digital options, interpreter services and trusted representative arrangements.

RECOMMENDATION 5. Government, together with industry, should fund First Nations financial counsellors, legal services and Aboriginal Community-Controlled Organisations (ACCO) to provide rapid, culturally safe assistance to scam victims.

RECOMMENDATION 6. The codes should require regulated entities to maintain culturally safe and accessible alternatives to digital self-service. This should include dedicated First Nations customer support, access to trained staff, interpreter services, assisted complaint pathways and arrangements for face-to-face or community-based support where digital engagement is not readily available. Having these services will give a practical reason for requesting a customer's First Nations status for better reporting and will be in satisfaction of Australian Privacy Principle 3.

RECOMMENDATION 7. Banks should be required to investigate the full cultural and practical context before relying on card, PIN or credential sharing to reject a claim. They should also explore with the customer and provide safer alternatives, such as culturally accessible account controls.

RECOMMENDATION 8. Scam warnings must be available in plain English and First Nations languages in accessible formats and should be developed together with First Nations organisations and communities. Information should also be delivered through trusted local channels such as ACCOs, Indigenous financial counsellors, local radio, community centres and face-to-face outreach.

RECOMMENDATION 9. At a minimum, the SPF should require staff who make scam-prevention, account-restriction, complaint or compensation decisions to be trained to recognise structural and service-access barriers experienced by First Nations consumers, understand culturally specific approaches to sharing money and resources, communicate through interpreters and culturally safe channels, avoid blaming or shaming consumers, provide trauma-informed assistance and appropriate referrals, and work effectively with ACCOs, First Nations financial counsellors and trusted support people.

RECOMMENDATION 10. Training content should be developed and reviewed with First Nations-led organisations. Regulated entities should also be required to measure training effectiveness, rather than merely recording staff attendance.

RECOMMENDATION 11. Under the SPF's respond pillar, regulated entities should be required to provide culturally safe reporting and complaint pathways, developed in collaboration with First Nations organisations and communities.

RECOMMENDATION 12. The SPF codes should expressly recognise First Nations community identification cards as an acceptable form of identification and require banks and other regulated entities to offer alternative verification pathways in compliance with AUSTRAC's guidance for identification.

If you have any questions about this submission please contact Pavithra Jayasekera, Policy Officer on 03 8554 6963 or at pavithra@consumeraction.org.au.

Yours sincerely,

CONSUMER ACTION LAW CENTRE

Jean Skeat

Jean Skeat | Director of Policy and Campaigns