NICE Actimize

Insights Article

The 2026 Status of the Australian Scam Prevention Framework

In 2025, the Australian Scam Prevention Framework (SPF) was hailed as a groundbreaking "first in the world" solution to help reduce consumer scam losses. This was the first time banks, telecom providers and digital platforms would be required to implement sound controls to help prevent consumer scams – and without those controls in place, they could face fines and be obligated to reimburse affected consumers.

Nearly a year later, Australians are waiting to see what the implementation of this legislation will look like. This article breaks down what has happened since the bill passed, outlines the proposed rollout and highlights where critical gaps still remain.

Background

In February 2025, the Australian Parliament approved the SPF. This legislation requires regulated entities, such as banks, telecom providers and digital platforms, to have controls in place to help prevent consumer scams.

The legislation is based on six key pillars:


Governance


Detection


Disruption


Prevention


Reporting


Response

If proper controls are not in place, banks, telecom providers and digital platforms can face fines of up to AUS $50 million or as much as 30% of revenue. They may also be required to reimburse consumers for any scam-related losses.

The SPF will have both an Internal Dispute Resolution (IDR), managed by the individual entities involved in the scams, and an External Dispute Resolution (EDR) process. The EDR will be run by the Australian Financial Complaints Authority (AFCA).

Current Status

In November 2025, the Australian Treasury released its consultancy outlining the proposed deployment of the SPF. The document defined the required controls for banks, telecom providers and digital platforms, including detailing how these entities would be expected to self-certify their compliance with those controls.

Here are some well-defined examples of the detailed controls:

1. Businesses must embed responsibility for scam prevention within their governance frameworks, including strategic risk management and oversight.
2. Businesses must identify and verify new users of regulated services.
3. Digital platforms must verify that advertisers hold the appropriate licenses to promote high-risk products, such as financial services and healthcare offerings.

In other cases, the controls are outlined at a higher level:

1. "Reasonable steps involve businesses taking genuine, proactive and proportionate actions to reduce scam activity on their platforms or services. These actions should reflect the size of the business, its operational complexity and exposure to scam-related threats."
2. "Larger businesses or those facing higher scam risks may be expected to go beyond minimum requirements to meet their obligations under the SPF."
3. "Sector codes will serve as the primary factor for assessing whether a business has taken reasonable steps. Other relevant factors include the size of the business and the kind of service involved in the scam."

The document excluded a number of entities, including:

- Non-bank payment services providers
- Cryptocurrency exchanges
- Crypto ATMs
- Online marketplaces
- Dating apps
- Email services
- Standalone generative AI services

The consultancy makes it clear that receiving banks are now included in the SPF. It also outlines how reimbursement is expected to work, though many questions remain unanswered.

The plan is for the SPF to partially launch on July 1, 2026, with IDR coming first, EDR beginning on January 1, 2027, and full deployment following later in 2027.

Outstanding Issues

One of the biggest issues is the large number of entities excluded from the SPF. This alone could significantly reduce the potential amount of scam loss reimbursement – for example, when a scam begins on an online marketplace and the payment is made via a non-bank payment service provider, there will be no reimbursement. Why non-bank payment service providers, online marketplaces and dating apps are excluded is quite puzzling, as these are major points where scams commonly occur.

Another key issue is that entities are responsible for determining their own compliance with the controls. This self-assessment approach puts Australian scam loss victims at a disadvantage.

A third issue centers on the weak definition of the controls. There is valid concern that banks, telecom providers and digital platforms could implement only minimal measures and still claim compliance, while consumers continue to lose billions to scams.

The Consumer Action Law Centre, an Australian consumer support group, echoes this concern. In its response to Treasury, it states: "The proposed multiparty Internal Dispute Resolution (IDR) model is unworkable and risks leaving victims to navigate complex processes alone," and warns that "some of the biggest platforms enabling scam activity are left untouched."

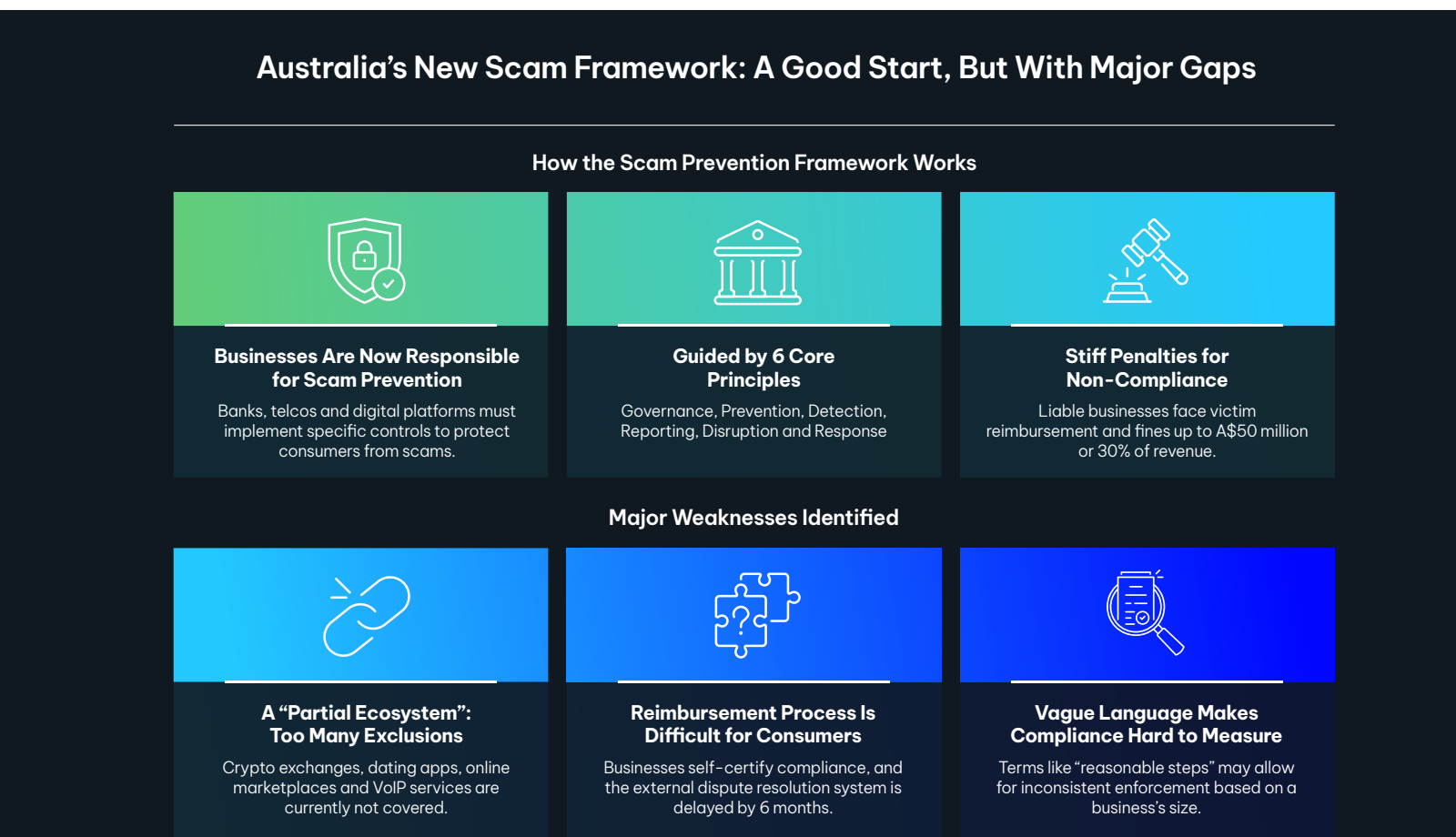

Figure 1 Current Status of the SPF

Summary

The Australian SPF is indeed a bold initiative. For the first time, banks, telecom providers and digital platforms are being brought together in a coordinated effort to combat consumer scams. However, the SPF also highlights the practical difficulty of linking scam-prevention controls directly to consumer reimbursement. Because the two are tied so closely, defining and implementing the controls has taken considerable time — during which consumer scam losses have continued to rise.

The controls and the reimbursement process must roll out simultaneously. As a result, some of the strongest and most effective controls, which could materially reduce scam losses, may not be included because they are more complex to define and measure. In addition, each control must be measured with enough precision to determine compliance or non-compliance, a critical factor in whether reimbursement will occur.

Australian consumer groups are increasingly concerned about how, or even whether, reimbursement will ultimately be delivered. While the government has promoted both scam controls and reimbursement as part of the SPF, the Treasury's consultancy document leaves significant questions unanswered. AFCA, as the External Dispute Resolution body, will face intense pressure. Yet under the current proposal – lacking clear control definitions and allowing entities to self certify – it will be challenging for AFCA to operate an effective EDR model. Ideally, these issues can be addressed quickly.

Given where the Treasury stands today (as of February 2026, having only recently received responses to the November consultancy), it appears more likely that the SPF's launch will be delayed until 2027. It is expected that Treasury will produce additional SPF content in March 2026.

Since 2005, Ken Palla has been in Online Security. He was a Director at MUFG Union Bank, retiring in early 2019. At MUFG Union Bank he managed the online security for both commercial and retail customers. Ken was an advisor to the RSA eFraud Global Forum and a Program Committee member for the annual San Francisco RSA Conference. In 2019, he received the Legends of Fraud Award. He has published many white papers—on the need to focus on online customer safety, on online authentication and on how to select a multi-factor authentication solution. Most recently, he has been writing about consumer financial scams and how around the world financial institutions are adding scam controls and sometimes providing reimbursement. He is currently consulting to banks and to online security vendors and is a member of The Knoble Scam Committee.