# Ping Identity Response to the Review into Open Banking

*Mark Perry, APAC CTO, Ping Identity*

*23 March 2018*

## Summary

Ping Identity ("Ping") is pleased to submit this response to the Review into Open Banking in Australia, released in February of this year.

We welcome this important document and on the whole, agree with its recommendations. We believe it is the beginning of a process that will set the course for secure digital interaction between service providers and application developers well beyond its initial scope of financial services in Australia, and as such, is a fundamental building block for Australia's digital future: enabling secure, consent-driven open data services across all industries.

Our expertise is in the standards and technology necessary to successfully implement identity-based services at internet scale.

In this response, we draw on our experience in developing and implementing industry open standards like SAML 2.0, OAuth 2.0 and OpenID Connect 1.0, the latter two being the security foundation of the UK's Open Banking protocols.

Ping's technology was selected by the UK's Open Banking Implementation Entity to play a key role in the architecture: it underpins the Open Banking service that manages the registration process and lifecycle for Account Servicing Payment Service Providers (ASPSPs), Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs).

Ping's recommendations in summary:

1. We agree that the UK's Open Banking specification and the FAPI draft standard should be the starting point for discussions on an Australian standard.

2. The UK's model of an Open Banking authority as an "Address Book" of registered and accredited participants should be replicated in Australia.
3. An authentication API based on OpenID Connect should be made mandatory for Open Banking in Australia, preventing the use of "screenscraping" technology and credential replay.
4. As a result of recommendation 3, the "redirect model" of authentication should be the preferred model for Australia.
5. A model for end user consent is essential for building consumer trust in Open Banking and must be in place in some form for the initial rollout of any service based on an Australian Open Banking standard.

# Discussion of Recommendations

## Recommendation 5.2 - starting point for the data transfer standards

**Standards for the Data Transfer Mechanism**

*"The starting point for the standards for the data transfer mechanism should be the UK's Open Banking technical specification. The specification should not be adopted without appropriate consideration, but the onus should be on those who wish to make changes."*

Ping agrees with this recommendation. While the UK's Open Banking standards continue to develop, the fact that there is a specification that is being used by banks, financial institutions, Fintechs, and their customers should give Australia a headstart on its Open Banking initiative.

In particular, the OpenID Foundation's Financial Application Programming Interface (FAPI), discussed briefly on Page 76 of the review , should provide the basis for discussions on the standard for the Australian data transfer mechanism, in Ping's opinion.

## Recommendation 2.9 — responsibility for the address book

*"Given that banking is a sector that requires accreditation, the regulatory framework needs to incorporate an address book for participants and customers to be able to know whether a party is accredited and the tier of accreditation held."*

Ping recommends the model used by the UK's Open Banking authority as an "Address Book" of registered and accredited participants (banks and financial institutions, and Fintechs, but not consumers). We believe this should be replicated in Australia.

In that model, interactions between consumer applications, and the banks and other financial services companies, are performed using the RESTful APIs standardised by Open Banking. Application flows don't force direct communication with the Open Banking "Address Book"; in this way the architecture avoids a single "clearing house" which could be a single point of failure or a honeypot for attackers, as pointed out on page 50 of the review.

The "Address Book" in the UK model also provides the digital certificates to secure the interactions between participants, removing the need for applications to exchange and

maintain digital certificates with each financial institution from which they consume services.

It also means that participants are free to choose the technology of their choice to implement their side of the Open Banking protocol conversation, not just that supplied by Ping Identity, something that has been overlooked or misrepresented in other organisations' previous submissions to the review.

## Authentication Experience

As specified on page **x** of the executive summary:

*Open Banking should not prohibit or endorse 'screenscraping', but should aim to make this practice redundant by facilitating a more efficient data transfer mechanism.*

In Ping's opinion, this recommendation could have gone further. Screenscrapers should be banned from replaying end user credentials to banking services. This practice is known in the IT Security industry as an "Anti-Pattern": something to be avoided at all costs.

The use of an Open Banking authentication API based on OpenID Connect should be mandatory.

Allowing screenscraping to continue only normalises a bad practice. Consumers are familiar with being redirected to another login screen to authenticate, for example, when they use social media services as an authentication authority for third party mobile and web apps.

This is touched on in the discussion of redirect and decoupled methods on Page 86 of the review.

*"The Data Standards Body should carefully weigh the merits of the redirect and decoupled models. However, the Data Standards Body should take into account that many open banking implementations already use the redirect model. Careful consideration would be needed before pursuing the decoupled approach."*

Ping recommends that the redirect model be mandated for Open Banking in Australia.

### Recommendation 4.5 - customer control

**End User Consent**

*A customer's consent under Open Banking must be explicit, fully informed and able to be permitted or constrained according to the customer's instructions*

The issue of informed consent is another important topic covered in the review. Consumers must at all times be aware to whom they are giving access to their data and how long that consent lasts, and they must be able to review and potentially remove their consent at a granular level at any time in the future.

A mandatory end user consent model will be a highly visible and ongoing way for consumers to trust Open Banking participants with their data, unlike one-time registration screens with onerous terms and conditions that are generally ignored.

## Conclusion

Ping Identity is excited for the future of Open Banking in Australia and will contribute our experience and know-how to help this important initiative move forward.

We believe there is an opportunity to enable secure open data services across all industries in Australia based on this work, which will ultimately benefit consumers as well as established and emerging companies, while safeguarding privacy and security.

We look forward to collaborating on this effort with the government, fellow IT industry participants including the Fintechs, third parties interested in consumer rights and privacy, and the financial services industry to build a solid, secure and consent-driven framework for Australia’s digital future.