Response to the Review into Open Banking in Australia

Australia Post
March 2018

auspost.com.au

Contents

1 Executive Summary 3

2 Key Feedback Summary 4

3 Digital Identity in the Financial Sector 5

4 Identity Standards 6

4.1 Government Standards 6

4.2 Financial Standards 7

4.3 Standards Required for Open Banking 7

5 Identity theft, identity providers and the overseas experience 9

5.1 Security Implications for Open Banking 9

5.2 Scandinavian Identity 9

5.3 Identity Provider Markets 10

6 Conclusion 11

1 Executive Summary

The Challenge of Digital Identity

Australia Post welcomes the opportunity to provide input into the recommendations of the Review into Open Banking in Australia (the Review). We are particularly interested in the reuse of identity verification checks, and this response is confined to the issue of digital identity management.

For over 200 years, Australians have been trusting Australia Post to securely deliver the sensitive information their letters and parcels contain. In our growing digital economy, Australians are now trusting Australia Post to securely deliver for them online including through banking, finance and identity services.

Our service offering online, particularly in digital identity, is growing quickly and utilises our physical footprint across the country. We have recently launched a reusable digital identity product for consumers, known as Digital iD™, which offers a secure digital alternative to prove an individual's identity and manage their personal information.

Australia Post also provides a variety of financial services, both directly and as an agent for, other institutions across Australia, and this exposes us to the importance of identity security. Through this activity, and also acting for government agencies, we conduct over 6 million identity checks each year.

Providing a reusable digital identity service to financial organisations has exposed us to many of the challenges facing the financial sector when it comes to secure online identity.

Identity Verification in Banking is generally done by individual organisations for a specific purpose, considered within a particular risk environment. The existing AML/KYC legislation gives organisations wide latitude to match the strength of an identity verification check with the level or risk identified by that organisation.

Open Banking challenges this model, as a second organisation relying on the identity verifications of a first may be operating in a completely different risk environment.

Further, traditional activity monitoring to identify suspicious behaviour will be more difficult, as the fraudulent activity may be spread across multiple institutions.

Privacy and security constraints that restrict the sharing of additional information, such as document identifiers, may also reduce the ability of relying parties to deduce the strength of the original verification.

Agreeing on common standards for identity verification checks can mitigate many of these problems and provide significant benefits to both customers and business. Overseas experience with programs such as the Norwegian "BankID" scheme have shown how the finance industry can significantly improve the ease and speed of consumer access to financial services with a high quality and secure shared identity.

The same overseas experience shows that when standard identity checks are combined with reusable credentials, and aligned with Industry standards, significant benefits can be achieved, not just for the finance sector but for the entire economy.

In addition to providing the enclosed input to the Review, Australia Post seeks to further engage the Attorney-General's Department on these issues of identity verification and security as part of future consultation rounds for the AML/CTF reforms.[1]

[1] Australian Government Attorney-General's Department, AML/CTF statutory review implementation, at https://www.ag.gov.au/consultations/pages/amlctf-statutory-review-implementation.aspx

2 Key Feedback Summary

The following summarises our feedback on the Report's recommendations:

1. Re 3.4: *Establish standards for identity verification*

Financial Institutions need to be able to rely on the strength of an identity verification performed by another party. The Review should establish a commonly understood baseline standard (compatible with AML/KYC legislation) for an identity verification, suitable not just for the transaction at hand, but reusable for future transactions.

2. Re Table 3.1, and 3.4: *Define levels of identity verification*

The Review lists a broad range of financial products, and suggests that post implementation "the potential for future write access" be considered.

Different products and access levels require different levels of identity security, so the Review will need to either establish a common high-standard suitable for all financial products, or define two or more verification levels of a commonly understood quality.

3. Re 5.2, 5.4: *Consider reusing or extending existing standards*

The Review suggests reusing UK standards, however existing identity standards across the UK and Australia are already well aligned. In establishing financial identity standards, existing systems such as the local National Identity Proofing Guidelines (NIPG) from the Department of Home Affairs, and the TDIF from the Digital Transformation Agency, should be considered, as well as engaging with AUSTRAC with respect to the direction of future AML/KYC legislation.

4. Re 5.5: *Match authentication strength to identity strength*

A common feature of existing standards is that a stronger verified identity can only be used as such if accompanied by an appropriate strength of authentication credential. If multiple levels of verified identity are used, they should be accompanied by authentication credentials of corresponding strength – e.g. 'read/write' credentials would need to be significantly stronger than 'read only' credentials.

5. Re 1.1, 3.11, 3.12: *Encourage a market for identity providers*

To encourage high quality service provision, the Review should encourage a market for specialist identity providers, and allow such providers to charge reasonable fees for the provision of such services.

Additionally, organisations that provide both financial and specialist identity services should not be prevented from commercialising their identity services due to having financial operations.

6. General Feedback: *Consider Identity in the workshops process*

The details of managing a reusable, shareable digital identity merit explicit consideration within the Review's standards workshops, either as a separate stream, or within one of the existing streams, such as the security group.

3 Digital Identity in the Financial Sector

Existing identity verification is largely focussed on identity proofing customers within a particular organisation, with that organisation choosing a verification process appropriate to the level of financial risk. The organisation can then monitor the activity of the customer, and increase the strength of the verification as required, such as when a savings account customer chooses to take out a home loan.

Financial institutions also have obligations within the scope of AML/KYC legislation, however the AML/KYC legislation also considers identity checks to have a certain level of risk, with options such as the "Safe Harbour" rules only applying at low and moderate levels of risk.

However the risks change significantly when we consider reusable identity. Open Banking envisions organisations relying on each other's identity verification checks in order to reduce friction for a wide variety of consumer activities. This may be problematic, as the relying organisation may not know the strength or manner of the original verification or the purpose for which it was made, and tracking suspicious activity between organisations will be more difficult - problems that currently constrain reliance on AML checks between institutions.

This implies that more rigour may be needed in the initial identity check, as a relying institution may not know whether an individual identified by a third party was checked to a degree appropriate to their current risk level. As an example, the various financial products listed in Table 3.1 have different levels of risk; a debit card account is generally lower risk than a high limit credit card account.

Further complexities arise when we consider the future of Open Banking, which will need to include partial and full delegation, read/write access, and the corresponding level of identity checks required for parties trusted with the management of accounts and funds.

A final issue is the changing nature of online security, as Identity Theft becomes more common and the ease of obtaining false documentation on the darknet, or even on public websites, becomes ever greater.

In the absence of common standards, legal and financial risk is likely to lead to Open Banking participants needing to frequently re-identify users, creating significant friction and undermining the core goals of Open Banking of customer control of banking.

Key feedback:

- Re 3.4: *Establish standards for identity verification*
  - Financial Institutions need to be able to rely on the strength of an identity verification performed by another party. The Review should establish a commonly understood baseline standard (compatible with AML/KYC legislation) for an identity verification, suitable not just for the transaction at hand, but reusable for future transactions.
- Re Table 3.1, and 3.4: *Define levels of identity verification*
  - The Review lists a broad range of financial products, and suggests that post implementation "the potential for future write access" be considered.
  - Different products and access levels require different levels of identity security, so the Review will need to either establish a common high-standard suitable for all financial products, or define two or more verification levels of a commonly understood quality.

4 Identity Standards

There are a number of identity standards currently used in Australia, with two major distinct 'groups' of standards being the Government's Identity Standards, and the AML/KYC standards used by the Finance Sector.

4.1 Government Standards

Current Government Identity Standards in the Anglosphere (UK, US, Canada, Australia, NZ) and ISO standards (e.g. ISO 29003 and ISO 29115) generally revolve around a number of discrete "Identity Proofing Levels", usually ranging from Level 1 (weakest) to Level 4 (strongest), with some minor variations (e.g. US NIST SP 800-63 combines level 3 and 4, while UK RSDOPS numbers levels as 0 – 3).

Most of these standards share a number of common principles or goals to guide the process of checking identities. In Australia the following principles from the "National Identity Proofing Guidelines" (NIPG[2]) are widely used in Government:[3]

1. **Confirm uniqueness of the identity in the intended context** to ensure that people can be distinguished from one another and that the right service is delivered to the right person. This reduces risks such as doubling up on service provision, however, whilst it may be unique in the context of the online transaction it does not necessarily need to uniquely identify the subject in all contexts;

2. **Confirm the claimed identity is legitimate** to ensure the identity has been genuinely created as well as confirming that there is continuity in a person's identity attributes where there have been changes. Increased confidence in the legitimacy of an identity is achieved through verifying Commencement of Identity evidence back to authoritative sources and verifying Linking Documents where name or date of birth details differ between pieces of evidence. This reduces risks such as the registration of imposters or non-genuine identities;

3. **Confirm the binding between identity attributes and the person claiming the identity** to provide confidence that the identity confirmed through objectives 1 and 2 is not only legitimate, but that the person currently claiming the identity is its legitimate holder. This reduces the opportunity for identity fraud. The Trust Framework relies heavily on facial binding to reduce this risk;

4. **Confirm the operation of the identity in the community over time** to provide additional confidence that an identity is legitimate in that it is being used in the community (including online where appropriate). Requiring a pattern of usage over a period of time implies that the identity has a history and reduces the risk that it is fraudulent; and

5. **Confirm the identity is not known to be used fraudulently** to provide additional confidence that a fraudulent (either fictitious or stolen) identity is not being used. Such checks, either internally or with external sources, such as law enforcement agencies or comparing personal attributes against the Fact of Death file decrease the risk of a fraudulent identity within the Trust Framework.

The degree to which these principles are satisfied determines the level of the identity check – for example at "level 2" the simple possession of a couple of documents (e.g. a driver's licence and a Medicare card) may be sufficient, at "level 3" a facial match might be performed against the driver's licence, and at level 4 an in-person interview is required.

The NIPG standard defines general principles for identity checks for government organisations, however there is still significant scope for different implementations of those checks, which make the sharing of Identity checks difficult. The fact that a user has identified themselves to the Department of Human

[2] Attorney-General's Department, 2016, 'National Identity Proofing Guidelines (NIPGs), Australian Government. https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/NationalIdentityProofingGuidelines.PDF

[3] Note that some elements, such as uniqueness, may not be appropriate to Industry.

Services, for example, does not automatically mean that the same identity check will be accepted by the Taxation Office.

In part to meet this requirement for a more specific standard to allow reuse and interoperability, the Government's Digital Transformation Agency has published the "Trusted Digital Identity Framework", or TDIF[4], which provides more concrete rules for identity verification, matched with authentication and risk standards, with the goal of creating an ecosystem of digital identity providers, both government and private, that can provide identity services to citizens usable across a wide range of government agencies.

4.2 Financial Standards

Current AML/KYC legislation provides a number of options for financial institutions to identify customers, and they provide significant latitude to providers to make risk assessments as to the depth of the identity verification required.

In particular, AML/KYC provides the "Safe Harbour" rule for identity verification, where for medium and low risk transactions a basic online check of two identity sources is usually sufficient to meet the requirements of the Act. Organisations are free to design their own verification processes however, which will take into account the specific risk profile of the organisation and the customer relationship being entered into.

Unfortunately, as noted in the Review into Open Banking in the context of the energy sector[5], organisational identity checks are not easily reusable, as different organisations have different requirements and different risk profiles.

While the AML legislation makes some mention of reuse, in practice this has been hard to achieve and only occurs after careful negotiation and comparison between organisations. While AML legislation acknowledges the possibility of verification sharing between organisations, it does not strongly consider the possibility of system-wide checks for reusable identity or the legal and risk impediments to doing so.

A further challenge is matching individuals between organisations. Many financial firms have struggled to provide an internal "single view of customer"– the problem becomes more acute matching users between multiple independent organisations.

4.3 Standards Required for Open Banking

Enabling reuse of Identity is fundamental to Open Banking. Consumers must be able to conveniently prove their identity once, and have that identity trusted by all participants. This requires participants to have a common understanding of the strength of the original identity verification, as well as the level of authentication and authorisation security.

As part of setting these standards, the Open Banking review should:

1. Create (or adopt) a standard framework for identity verification;

2. Carefully define the difference between identity verification, authentication, and authorization to avoid confusion between participants and clarify roles;

3. Include standards for verification with either a single, strong verification level suitable for all purposes, or a discrete number of levels with usage guidelines;

4. Set minimum security and privacy related requirements to avoid a race to the bottom on risk, quality and cost;

[4] Digital Transformation Agency February 2018: https://www.dta.gov.au/what-we-do/policies-and-programs/identity/

[5] Open Banking Review p.20: "*Currently third-party providers in the energy sector need to negotiate bilaterally on identity confirmation and data access processes with every distributor.* "

5. Encourage changes to AML rules to encourage alignment, reducing compliance costs and improve efficiency;

6. Consider the Governments TDIF standard, and potentially additional granularity at lower levels to accommodate the needs of the financial services sector; and

7. Suggest a certification approach be undertaken so others can rely on Identity Verification both from other institutions and third parties.

Key feedback:

- Re 5.2, 5.4: *Consider reusing or extending existing standards*
    - The Review suggests reusing UK standards, however existing identity standards across the UK and Australia are already well aligned. In establishing financial identity standards, existing systems such as the local National Identity Proofing Guidelines (NIPG) from the Department of Home Affairs, and the TDIF from the Digital Transformation Agency, should be considered, as well as engaging with AUSTRAC with respect to the direction of future AML/KYC legislation.

- Re 5.5: *Match authentication strength to identity strength*
    - A common feature of existing standards is that a stronger verified identity can only be used as such if accompanied by an appropriate strength of authentication credential. If multiple levels of verified identity are used, they should be accompanied by authentication credentials of corresponding strength – e.g. 'read/write' credentials would need to be significantly stronger than 'read only' credentials.

5 Identity theft, identity providers and the overseas experience

5.1 Security Implications for Open Banking

Identity Theft is becoming a rapidly increasing problem[6], and the current AML/KYC Safe Harbour rules may no longer be strong enough for a reusable identity, where the existing controls financial institutions can exert over fraudulent behaviour may be weaker.

The difficulty of using the existing AML/KYC rules in a multi-organisation environment can be seen by comparing them against the NIPG guidelines:

1. Under AML, when an identity is used across multiple organisations, it is difficult to establish uniqueness as name and date of birth may be insufficient;

2. AML Safe Harbour rules are becoming less effective given the ease of creation or purchase of false credentials;

3. AML/KYC has no requirement for 'binding' the credentials to the use (e.g. by facial matching with photo ID), exposing organisations to some classes of identity fraud;

4. AML has some guidance about checking a customer history over three years, but this is optional and organisation specific; and

5. Fraud checks, and checks of Politically Exposed Persons, are not standardised.

If Open Banking is going to make use of reusable identity verification, and create an environment where institutions can trust an external verification without making additional checks, there will need to be a common understanding, and a common standard that tightens up these issues to reduce systemic risk.

It is also worthwhile considering the changing threat environment, as false credentials become more widely available, and the cost of stolen documents and document details falls. These threats are being addressed in other areas with new security controls such as automated biometric facial matching systems, and the increased ease of checking an ever increasing range of documents back to their issuing bodies.

Specifically, the Review should note the work done by the Facial Verification Service ("FVS") of the Department of Home Affairs, which allows for automated facial comparison against reference photos held on passports, visas and driver's licences, and also the similar work done by identity providers such as Australia Post in high security facial comparisons against the electronic version of facial images held on ePassport chips.

5.2 Scandinavian Identity

A number of international examples exist of reusable identity within the banking sector. The Review has already mentioned the UK, however there have been some difficulties with customer adoption that are still being worked through.

An example of a healthy shared financial identity is found in the Norwegian "BankID" environment[7], and the similar service in Sweden. The Norwegian service has been in operation for over ten years and is now used by over 70% of the Norwegian population, including the vast majority of working age adults. Significantly, the service is also used for government services, providing significant user utility. However while the service was promoted and supported by government, it was largely driven and implemented by the financial sector, and the finance sector continues to account for the majority of services.

[6] "Identity theft has never been more rampant" CBS News, Feb 6 2018 https://www.cbsnews.com/news/identity-theft-hits-record-high/

[7] BankID Home Page: https://www.bankid.no/en/about-us/

In Sweden where a similar "Mobile BankID" scheme operates (65% penetration) more than 90% of the usage of the service is financial. The success of the service is attributed to ease of enrolment, the support of government, and the co-operation of a council of leading financial institutions.

5.3 Identity Provider Markets

A common feature of these systems is that not every relying party is an identity provider. Identity providers that can provide identities for an entire system or country are generally held to a higher standard than in-house organisations, and require specialist legal, fraud, security and IT skills. Requiring this standard from all participating institutions may limit the number of possible contributing entities and act as a barrier to entry for new market participants.

Specialist identity providers are appearing and competing in other contexts (such as identity provision for government and health services), leading to innovation, better security, improved customer service and lowering the costs of identity verification.

Independent identity providers may also be in a better position to manage the full identity lifecycle including digital identity issuance, recovery, renewal and disposal, and to better assist users with managing identity theft, which impacts their relationship with not one, but a large number of organisations.

Market based solutions will need to allow providers to compete on both quality and price. Australia Post notes the review recommendations that data be transferred free of charge, and specifically that identity verification results be transferred free of charge (3.11).

We believe this would have the unintended consequence of preventing the reuse of existing identities from outside the finance sector (such as high quality government digital identities under the DTA's TDIF system). It may also inhibit a consumer facing market of 'trusted third party identity providers' that act on the customer's behalf, independent of the potentially conflicting incentives of financial service providers.

A further distinction should be made where organisations provide both financial services and other services (such as specialist digital identity services). It should be explicit that providing financial services in one part of an organisation does not prevent that organisation providing and charging for specialist identity services. A large number of current and potential identity providers are insurance companies, telecommunications companies and postal organisations, which provide a range of services that may extend well beyond financial services.

Key feedback:

- Re 1.1, 3.11, 3.12: *Encourage a market for identity providers*
  - To encourage high quality service provision, the Review should encourage a market for specialist identity providers, and allow such providers to charge reasonable fees for the provision of such services.
  - Additionally, organisations that provide both financial and specialist identity services should not be prevented from commercialising their identity services due to having financial operations.
- General feedback: *Consider identity in the workshops process*
  - The details of managing a reusable, shareable digital identity merit explicit consideration within the Review's standards workshops, either as a separate stream, or within one of the existing streams, such as the security group.

6 Conclusion

Australia Post welcomes the opportunity to provide input into the recommendations of the Review, particularly focused on identity verification.

The establishment of Open Banking standards is a significant opportunity to lift the efficiency and convenience of the financial sector.

Providing a commonly understood, reusable standard for consumer identity is not only a prerequisite for Open Banking, but based on overseas experience may have wider benefits for consumers, helping to digitise other areas of the economy such as health care and government, and simplifying transactions between these sectors.

Correctly implemented, it will provide an appreciable boost not only to the financial sector, but to the Australian economy as a whole.

Australia Post looks forward to working together with Government, industry and consumers to further develop and implement Open Banking standards in the near future. This includes seeking to work with the Attorney-General's Department on these issues of identity verification and security as part of future consultation rounds for the AML/CTF reforms.