[redacted]

Thank you for the opportunity to provide feedback on the Federal Government's Digital ID framework.

Bendigo and Adelaide Bank is Australia's most trusted bank with more than 2.4 million customers and 8,000 staff across Australia. Our vision is to be Australia's bank of choice, driven by our purpose to feed into the prosperity of our customers and communities, not off it. This purpose underpins everything we stand for and the actions we take. We believe our success is driven by helping our customers and the communities in which they operate, to be successful.

Our Bank is proudly digital by design, but human when it matters. We have a long and strong record for innovation, agility and delivering customer-led solutions. Alongside our purpose driven culture and strategy, these strengths enable us to be nimble and quickly adopt industry-leading practices that benefit our customers.

A federal digital identity framework has the potential to bring widespread social and economic benefits with enormous opportunity to strengthen customer protection and improve business efficiency. With the proliferation of scams, our Bank, along with the rest of the industry, have significantly invested in technologies to better protect consumers against cyber fraud. Our Bank believes Digital ID will provide an important safeguard in protecting customers. This will only be realised where the benefits can be accessed Australia-wide. Therefore, we urge the government to take further consideration for improved accessibility for vulnerable and special-interest consumers.

We are pleased to contribute to the national conversation about Australia's digital identification framework and broadly welcome this important reform.

[redacted]

Registered head office
The Bendigo Centre
Bendigo VIC Australia 3550
Telephone: 1300 236 344
+61 3 5445 0666 (overseas)
www.bendigobank.com.au

Bendigo and Adelaide Bank Limited
ABN 11 068 049 178
AFSL 237879

About Bendigo and Adelaide Bank
Bendigo and Adelaide Bank is an ASX200 listed company with more than 8,000 employees who support over 2.4 million customers around Australia to achieve their financial goals. Our Bank has assets under management of more than $90 billion, a market capitalisation of over $5 billion and more than 110,000 shareholders across Australia. Bendigo and Adelaide Bank Group is the corporate entity for a network of brands including Bendigo Bank, Rural Bank and Up.

Our Bank is the only regionally headquartered ASX listed financial institution with more than half our branches situated in rural or regional settings. Our vision is to be Australia's bank of choice, and we believe our success as one of Australia's biggest banks is driven by our purpose – to feed into the prosperity of our customers and communities, not off it**.**

Role of Digital ID for financial services
Bendigo and Adelaide Bank welcomes the Government's framework for widespread adoption and use of digital identification through an evolution of the current Trusted Digital Identify Framework (TDIF).

A robust and well-designed framework for digital identification will bring strong productivity growth across the economy. For the financial services sector, widespread adoption and use will enhance our customers' experience and allow for faster access to banking services through improved identification speed. It will also reduce the need for paper-based identification which can be at higher risk of being lost or stolen. For our customers, Digital ID will reduce the time, effort, and expense that sharing physical documents can take when people need to provide legal proof of who they are, for example when buying a home or starting a new job. Simultaneously, the reforms will offer the best opportunity to address fraud and cyber security issues.

The success of the Government's Digital ID scheme will be judged against the take-up of the scheme, which ultimately is informed by consumers' trust in the scheme. With this in mind, our Bank applauds the Government's careful and sequenced approach to implementing the scheme.

Business customers

For the financial services sector, the benefits of the Digital Identity scheme will be fully realised when digital identification services have been successful and fully rolled out across the economy. As a bank, verifying a customer's identity is just one part of our identification management process; our staff must also verify a customer's relationship to an asset, a business or another person. We would welcome greater consideration of how Digital ID can interact with other government databases to allow customers to prove their relationships with assets, businesses and other individuals. Such consideration would be particularly beneficial for our business customers who may need to prove ownership of a business.

The Australian Taxation Office currently uses its in-house program, Relationship Authorisation Manager (RAM), to authenticate business clients and link it to a personal GovID account. We encourage the government to connect Digital ID to the RAM software, or a similar program, as an authentication for business customers and add business customers to the digital verification phased roll out. Our Bank would encourage this to be part of phase three.

Accreditation

Trust is a cornerstone to the success of the financial services sector and maintaining consumer trust is of the utmost importance to our organisation. A well-designed digital identity accreditation and operating framework will strengthen consumer trust through enhanced protection of consumer's personal information. Trust will be built by consumers having a consistent positive experience through consistent assurances of privacy and data protection. Therefore, in choosing a digital service provider, our Bank will need to guarantee the highest security and privacy standards needed to use digital identities.

Noting this, our Bank welcomes the flexibility that's built-in to the legislative provisions governing the TDIF. This flexibility will ensure that accreditation requirements can adapt as fraud and cyber risks evolve. The rules around the accreditation process provides sufficient guarding against scam and fraud risk. However, we consider there may be a risk associated with the onboarding of new accredited digital providers, following the accreditation process. It is our view that the management of collective risks and events will need to drive changes to the TDIF. On this basis, our Bank recommends that the Government undertake regular reviews of digital service providers and incorporates a dispute resolution process managed by the regulator to allow customers to raise concerns about digital providers.

Recommendation 1: Undertake regular reviews of the digital service providers and incorporate a dispute resolution process.

Recommendation 2: The government to connect Digital ID to the RAM software, or a similar program, as an authentication for business customers and add business customers to the digital verification during phase three of the roll out.

Addressing scams and cyber fraud in financial services

Consumer trust plays a significant role in our social licence to operate. With the proliferation of scams impacting our customers, our Bank, along with the rest of the financial service industry, have introduced a number of security enhancements to better protect our customers against cyber security risks. The introduction of Digital ID will add another tool for companies to use to mitigate the incidents of cyber security fraud and scams. With this in mind, we have detailed considerations to strengthen the framework's ability to limit cyber fraud across the digital ecosystem.

Operation of the Digital ID application

Our understanding of the Digital ID process is that once a service (like a bank) requests identity authentication, a digital identity service provider will prompt the customer to confirm a one-time passcode to verify their identity against secure database(s). While OTPs are generally considered a more secure method of connecting to services, our recent experience has seen impersonation scammers requesting customers to willingly share their OTP with the scammer, despite our best efforts to educate customers about the risks. Our Bank recommends a well-resourced digital literacy campaign alongside the roll-out of Digital ID that provides resources on keeping customers safe against scams and fraud, including the dangers of sharing a one-time password and other credentials.

Further, we are concerned about the potential for a scammer to sign up victims to a number of different digital identity providers with stolen credentials. Therefore, it is important that consumers can quickly and easily find and disable access to digital providers that they haven't themselves signed up to. We encourage the Government to consider how individuals can easily view and delete, or limit access to, digital providers in one place, such as an individual's MyGov account which could display which digital ID service providers an individual is signed up to, and a log of where their digital ID has been used.

Biometric data

Our Bank welcomes the inclusion of biometric data into the Digital ID framework. While digital identification will be useful in mitigating scams and fraud, the inclusion of access to biometric information provides an unprecedented opportunity for organisations like ours to detect and prevent fraud.

While we acknowledge that various stakeholders hold legitimate privacy concerns about biometric data being used in this way, we believe it is possible to strike a balance between the privacy interests of individuals and ability for relevant organisations to use this data to protect against criminal activity.

Our Bank would welcome further thinking around isolated exemptions to providing biometric data to the private sector, on application to a regulator or the Minister, for the sole purpose of scam and fraud reduction.

Right to be deleted

Section 28 of the Digital ID Exposure Draft Legislation requires an accredited identity service provider to deactivate a digital ID of an individual on request by the individual. There is no definition of '*deactivate'* in the Exposure Draft Bill. It is our belief that on deactivation of a profile, access to a digital trail should remain on the digital provider's database, even temporarily. Without this, scammers could create accounts across different services, engage in criminal activity and then quickly deactivate their account leaving no ability to track and trace criminal activity. Leaving a digital trail, even temporarily, would help to quickly identify and shut down new accounts made under a fraudulent account. Blockchain technology is a potential solution to this.

Recommendation 3: A well-resourced digital literacy campaign alongside the roll-out of Digital ID that provides resources on keeping customers safe against scams and fraud, including the dangers of sharing a one-time password and other credentials.

Recommendation 4: Further thinking around isolated exemptions to providing biometric data to the private sector, on application to a regulator or the Minister, for the sole purpose of scam and fraud reduction.

Recommendation 5: Access to a digital trail should remain on the digital provider's database, even temporarily.

Vulnerable and Special Case Customers

Our Bank welcomes the opportunity to improve financial inclusion with the roll out of a federal digital ID. We consider that, on the whole, the Digital ID framework will allow vulnerable customers to enjoy easier access to financial services. However, we have provided some examples of customers that will require deeper consideration by the Government to ensure optimal accessibility to the scheme.

Rural and Remote Customers

As Australia's economy becomes increasingly digitised, there are significant barriers for people living in parts of rural and remote Australia which could continue to challenge their ability to fully participate in the economy. Digital accessibility issues across regional and remote Australia are well documented, with access to reliable, high-speed internet being most prominent. Alongside a government-led push for Digital ID take up, we urge a continued focus to address significant mobile black spots and internet connectivity enhancements across rural and remote parts of Australia.

Power of Attorney

Within the financial services sector, there are strict requirements for dealing with customers with Power of Attorney status, such as identification and verification processes and documents. Customers with a Power of Attorney order in place are at increased risk of experiencing financial abuse, and therefore we place a higher level of scrutiny on the relationship to ensure the safety of the customer.

In the operation of Digital ID, we recommend the Government consider a way to link a Power of Attorney agreement between two digital ID profiles to create simplicity in proving that a Power of Attorney relationship exists.

Minimum age requirements

When considering a minimum age requirement for the digital verification services, it's important to be aware of the current processes for opening a bank account for minors and dependants. In the case of a minor, a parent or caregiver will need to prove the identity of the minor and their relationship to the parent or caregiver to be able to open a bank account. Generally, this requires paper copies of birth certificates, drivers' licences and any other identification for both the minor and their guardian. This is then verified by staff before a bank account is opened. Of course, there will be other situations where guardians may need to provide identification for their dependants, such as medical and education related events.

While we understand the government is considering an appropriate minimum age for access to digtial identification, the above processes may be more difficult for those under a minimum age. A minimum age cut-off would require organisations to maintain dual processes for both digital ID verification and paper-based ID verification, eroding any productivity and privacy gains made by introducing Digital ID. Therefore, our Bank urges the government to consider the implications of not allowing minors to sign up for digital identification and consider different options, such as linking a parent or caregiver's Digital ID to their children's for ease of access to various services.

Recommendation 6: Continued focus to address significant mobile black spots and internet connectivity enhancements across rural and remote parts of Australia.

Recommendation 7: Further thinking about linking a Power of Attorney agreement between two digital ID profiles to create simplicity in proving that a Power of Attorney relationship exists.

Recommendation 8: Further consideration of implementation options for minors to take advantage of Digital ID services.

Sector-wide digital verification

The Digital ID framework articulated throughout the consultation phase allows for a Digital ID marketplace with many different digital service providers and accredited service providers. This could lead to a proliferation of digital providers, some who are trusted, accredited providers and others who are not. It is our view that this could lead to greater confusion among customers.

Our Bank also holds competition-related concerns that large, market-dominant organisations could set up their own digital ID service to attract and retain customers by increasing their 'stickiness' and placing another barrier in the way of customers looking to switch services.

We encourage the Government to facilitate a sector-by-sector digital service provider. This way each sector, or multiple sectors, can adopt a digital service provider to use for their services without confusing customers and impacting their ability to switch. This encourages interoperability between different sectors and service providers. Alternatively, we are open to the Government offering GovID as the preferred service provider.

Recommendation 9: Encourage the Government to facilitate a sector-by-sector digital service provider scheme.

Conclusion

A robust Digital ID framework has the potential to bring widespread social and economic benefit. We see enormous opportunity for both consumers and businesses through strengthened privacy settings, enhanced customer experience and improved business efficiency and productivity. As a bank, we also recognise the role Digital ID could play in combatting scams and financial crime. We urge further consideration for vulnerable and special-interest consumers to improve access and simplicity so that the full benefits of Digital ID can be realised Australia-wide.