29 July 2016

Data Availability and Use
Productivity Commission
GPO Box 1428
Canberra City ACT 2601

Dear Sir/Madam

Re: Productivity Commission Inquiry into Data Availability and Use

The Australian Payments Council (APC)[1] – the strategic coordination body for the payments industry – is pleased to provide this response to the Productivity Commission Inquiry into Data Availability and Use.

The future of payments is data rich and this presents significant opportunities for a wide range of organisations. However, the way payments related data is treated, stored and disseminated needs to be carefully managed; it must align considerations such as consumer protection, commercial incentives, security, privacy, compliance and liability.

As part of its mandate to maintain security and trust in the Australian payments system, the APC has undertaken to consider the requirements for a digital identity framework. Foundational work on this included the development of guiding principles for digital identity. These principles, developed in conjunction with over 40 organisations from the public and private sector, are designed to ensure the security and privacy of digital identities. They are grouped into three categories: regulatory, commercial, and technical.

In producing these principles, consideration was given to matters of access, security, customer control and convenience, standards and consumer education. It is in this context they are offered for consideration by the Productivity Commission.

The APC's digital identity principles are included as an appendix to this letter.

Should you have any questions, Damien Butler from the APC Secretariat is available to assist you.

Yours faithfully

Mark Birrell

Chairman

[1] The APC fosters the ongoing development of the Australian payments system to ensure it continues to meet the changing needs of Australian businesses and consumers with innovative, safe and competitive payment services.

Australian Payments Council: Digital Identity Principles

Promote Privacy	**Digital identity systems and services must promote the privacy of personal information.** Privacy is a fundamental human right. This includes the right to privacy of personal information. Personal information is wide ranging including basic details, financial, medical, biometric, preferences, usage and connection data. Data that is not by itself personal may become personal in aggregate. Digital identity systems must be designed to protect the privacy of individuals, who must be viewed as the owners of personal data pertaining to them. Identity and attribute providers will provide services to help individuals manage their data. This should apply to all providers not just regulated entities. Education of individuals on the value of their personal data and the need for privacy is vital. Industry too has a duty of care to protect individuals from actions that will undermine their privacy.
Give Individuals Choice	**Individuals must be able to choose between digital identity service providers and to use different providers for different purposes.** Individuals should be provided with meaningful choice of digital identity services. This choice must be based on a clear, transparent and understandable articulation of how personal information is collected, stored, used, shared and deleted. Individuals should be able to use different digital identity services for different purposes where appropriate. On the other hand, individuals must not be required to maintain multiple digital identities. The individual should be in control and encouraged to take responsibility. Service providers should be engaged to ensure both sides of the identity market (identity provision and identity acceptance) develop to offer meaningful choice which will foster innovation and discourage anti-competitive behaviour.

Australian Payments Council www.australianpaymentscouncil.com.au
Level 6, 14 Martin Place, Sydney NSW 2000 Telephone +61 2 9216 4888 Facsimile +61 2 9221 8057

Require Transparent Accountability	**Digital identity services must be shown to comply with appropriate and necessary standards reflective of the level of assurance and intended use of the digital identities concerned.** Assured digital identity services need to comply with a recognised set of rules that provide confidence in the processes employed, technology used and competence of the organisation concerned (a "Trust Framework"). These rules should cover the full identity lifecycle including enrolment, usage, revocation and reestablishment of compromised or corrupted identities. They should also define how services are shown to be compliant whether through external audit or self-certification. Appropriate governance arrangements will need to oversee the creation, management and implementation of Trust Frameworks. Systems should also be transparently secure wherever possible, minimising the need for trust in organisations.
Allow Flexible Disclosure	**Individuals must be able to minimise the personal data they share with third parties.** The amount of personal information that is required will vary from service to service. The data required to onboard customers may vary from the data required for subsequent service delivery. In some cases only specific attributes (or partial attributes) may strictly be necessary. In others it may be possible to provide part of a service based on a limited set of personal information and only to require additional information when necessary. For some services, the fact that an identity has been assured to some level (e.g. is known to an identity provider) may be sufficient. Within payments examples already exist (e.g. prepaid cards) for which lower levels of KYC are acceptable.

Enable Inclusive Access	**Digital identity should be designed to enable access to both digital and non-digital services.** Digital identity services should be designed to work seamlessly in digital and non-digital contexts. This should include web, mobile, voice and face-to-face. In the future it should include IoT, where devices are delegated to act on behalf of individuals. Digital identity should remove friction during onboarding as well as during ongoing authentication. This may include leveraging authentication technology available in mobile devices or using cloud-based analytics to detect and block fraudulent activity. Some level of friction may be desirable for digital identity services, to provide control and the assurance to the end user that security is in place. Services should be inclusive. In particular there may be a need to complement fully digital services with "assisted digital" services or non-digital services for the digitally excluded.
Use Open Standards	**Digital identity services and solutions should be aligned with open standards.** Digital identity services must be built on and promote using open standards including: • protocol standards (how systems talk to each other) • functional standards (provide consistent and comparable services) • security standards (standardised levels of assurance or alternatives such as "vectors of trust"). The open standards that are relevant will depend on the nature of the services being built but could include OpenID Connect, Oauth, SAML, UMA or FIDO. It may be appropriate for the payments industry (by itself or in collaboration with others) to establish a trust mark as a signal for users.

Be Convenient	**Digital identity services must be simple and convenient to use, working the same way across many contexts.** Digital identity services must not place unnecessary barriers between individuals and service providers, to ensure individuals can access legitimate services conveniently. A consistent user experience should be developed across service providers and identity providers to build confidence amongst users of digital identity services. Extensive user testing should be employed to ensure services provide the optimal experience. This should include testing user attitudes to using payment industry credentials for non-payments purposes. To avoid confusion, users should only be offered a choice of identity provider when the provider will be able to meet the requirements of the service provider. Convenience must be balanced against security. Services must be simple to use without lowering security.
Be Appropriately Secure	**Digital identity services must meet security requirements appropriate to their usage.** Digital identity services must have fit for purpose security for their intended use. This will require a risk based approach but ensure that the level of security employed is clear. This may be achieved through defined levels of assurance or alternatives such as “vectors of trust”. This will enable business stakeholders to ensure security employed meets business needs. The security of all aspects of the digital identity service, including processes employed and technology used, shall be considered. Security shall be viewed as separate from privacy. Privacy requirements should be met even if security is lowered, for example by allowing lower levels of authentication on certain transactions.

Ensure Commercials Support Privacy	**The commercial model for digital identity must support the privacy principles** The commercial model will be critical to the success and sustainability of any digital identity scheme. To date, many low assurance digital identity schemes have depended on collecting, analysing and sharing massive amounts of data. For high assurance, digital identity schemes and the associated commercial models should be chosen to promote good practice and an appreciation of the value of digital identity. The commercial models (especially how the identity provider or service provider make money) must not undermine privacy. This does not exclude the collection of data but any such collection should either be necessary for the delivery or improvement of the service, have clear benefits to the individual and be done with their explicit consent.
Enable Transparent Exchange	**The exchange of personal data for services or other value must be transparent to the individual.** The value to individuals of sharing their data may come in a variety of forms including increased service levels and greater convenience. This exchange must be transparent, ensuring that the individual is aware of what benefit they are receiving in exchange for their data, what benefit the service provider is receiving and the potential future ramifications of the exchange. A code of practice should be developed for data sharing. For digital identity services to be most effective, providers should avoid all or nothing scenarios where individuals are required to share maximum data or get no service. The value of data is not necessarily monetary. There may be a mutual benefit (to both the individual and service provider) in sharing data.

Provide Clear Commercial Benefit	**Digital identity systems should provide tangible commercial benefits over legacy systems.** For a digital identity system to be successful it must make commercial sense. The cost of using the digital identity must be matched by an appropriate set of benefits including: • Reduced costs through more efficient digital identity management. For banks this may include reduced KYC costs. • Reduced costs through increased use of more efficient online channels. • Increased revenue by enabling new services. There may be benefits both internally and externally in collaborating on digital identity. In the Australian market the less developed credit bureaux market may mean that sharing KYC has greater benefits than in other developed markets.
Build on Core Competencies	**Digital identity services delivered from the payments industry should build on the core strengths of payments providers** Payments networks can be viewed as "functional" digital identity systems. They provide digital identity and authentication services for the purposes of instructing payments. These capabilities position the payments industry to have a strong role to play in digital identity. Banks in particular have strong trusted relationships with individuals that could be the basis for providing trusted digital identity services. The payments industry learn from and build on earlier attempts to collaborate in digital identity.