



Finance Brokers Association of Australasia Limited
(07) 3847 8119 | fbba.com.au
Level 1, 1 Miles Platting Road, Eight Mile Plains QLD 4113
PO Box 4792, Eight Mile Plains QLD 4113
ABN: 22 094 784 040

Department of Finance
Australian Government
Submitted online

Verifiable Credentials – Consultation Paper Parts A and B

The FBAA welcomes the opportunity to provide a submission for the above consultation paper. Our submission will address select questions posed by the paper.

The FBAA represents more than 14,000 members in Australia. Our member base comprises mostly finance and mortgage brokers, various lenders, aggregators and businesses supporting the finance industry.

Part A Questions

- a. How might the adoption of VCs enhance economic efficiency and help to grow productivity in Australia? How are these effects distinguishable from other ways of accessing and using credentials?**

Finance and mortgage broking are heavily document and process dependent. Identity verification is an important step in any interaction with a customer. Brokers act as agents of designated services providers under AML/CTF legislation and commonly undertake verification of identity (VOI) procedures to assist reporting entities to discharge their VOI obligations under AML/CTF. Identity verification is currently addressed through a range of processes including face to face dealings, using services such as Green ID and following processes for virtual identity verification such as having customers hold up a copy of their licence in a photograph or taking a screenshot from within a video. Broker record keeping obligations require that they retain evidence of having undertaken VOI for a period of 7 years which results in records of customer identification being retained on the broker's systems and also made available to the lender.

Identity verification processes result in multiple customer identification capture points and multiple points of potential attack for identity theft and other cybercrime including at point of capture, in storage and in transmission.

When thinking about steps taken to verify identity, the collection and storage of personal information is undertaken as a record of evidence of certain inquiries having been made. The objective of identity verification is not to collect specific identity documents, but to prove that we are dealing with the individual(s) we believe we are. Where possible, we want to have processes that confirm the identity but which do not require collection, transmission and storage of personal information. Steps that can be taken to reduce or

eliminate the need to capture, store and transmit the personal information of a customer are welcome.

Brokers must manage the tension between Anti-Money Laundering compliance regarding identity verification and privacy. Efficient VC processes can boost economic efficiency where they result in immediate and easy identity verification and which eliminate unnecessary capture of a customer's personal information. If proof of identity verification could be created by code or token or some other form of electronic certification that does not require customer personal information to be stored and transmitted, this would relieve considerable compliance pressure on a wide range of customer-facing service providers.

b. What use cases for the adoption of VCs do you think are viable in Australia (from the perspective of both the issuer and the verifier)? Which of these do you think are the most valuable and/or important for the Commonwealth to explore?

Any situation where identity verification is a legal obligation to be discharged as part of providing a service. The Consumer Data Right (CDR) contains elements of efficient identity verification and we would expect that the development of verifiable credentials policy in Australia would draw on the experiences from those existing systems and processes.

i. What sorts of behaviour needs to be guarded against or encouraged in a broader VC system?

The risk of bad actors and exploitation increases where we move away from traditional face to face identification to other means. As we provide other pathways for people to interact with each other and businesses, we create opportunities for fraud through false identities and anonymity.

Unnecessary collection and storage of information creates vulnerabilities as that data is only as secure as the systems they are stored on. Too often, too much of one person's personal information is stored in a single location (for example, name, address, date of birth, email address and potentially other identity information) resulting in bad actors obtaining all of the information needed for identity theft when they gain access to such records. We need to move away from designing systems and obligations that result in personal information being gathered and stored in vulnerable settings. Whether digital identity processes can remain impervious to hacking and interference is a primary concern. Reducing the co-location of multiple points of personal information together with reducing record collection and storage must be a priority.

j. How can VCs help to improve the inclusivity of government services? Are there any potential barriers to inclusion that VCs might inadvertently introduce?

Age is a material barrier. Older Australians who do not interact in the digital world are becoming excluded. From something as simple as receiving a utilities bill to booking a doctor's appointment, for many older Australians it becomes too hard once they are required to use an app to make a booking or provide email and other personal details online. While it sounds simple, even retrieving a code sent by SMS can prove difficult. Older Australians are considerably more vulnerable to scams and this vulnerability is exacerbated when they are struggling with technology. It remains important to consider how an older Australian might interact with new processes and systems and to maintain support for traditional approaches that do not require technological competence.

Part B questions

We agree with the policy positions advanced in Part B. We recognise at this point in time that they are very high-level and will require significant development.

Having regard to the possible approaches for verifiers under 4.2.3, we would prefer to see a system that does not require registration or additional steps to become trusted verifiers if such can be avoided. Or, if it is required, that it only be required one time for each verifier.

We strongly encourage broad thinking on how identity verification can be undertaken and identity proven beyond traditional approaches of obtaining records, cross-checking information and storing those records together with the results as proof of what was done. This verifiable credentials policy work is an opportunity to initiate significant reforms to how identity is verified in the course of business services. With the recent AML/CTF Tranche 2 reforms coming online, even more entities are drawn into identity verification obligations and finding a single, streamlined touchpoint that discharges the obligations for all service providers rather than each having to verify identity every time could create enormous efficiencies.

The development of verifiable credentials policy and the processes and procedures that will flow from it will consume a large amount of resources from all impacted groups. We strongly encourage directing some of that effort into further thinking on how verification can be proven and a recoverable record created of the steps taken to prove a person's identity without the need to store physical records or copies of personal information.

**Finance Brokers Association of Australia
July 2026**

