AGL Energy Limited
T 02 9921 2999
F 02 9921 2552
agl.com.au
ABN: 74 115 061 375

Level 24, 200 George St
Sydney NSW 2000
Locked Bag 1837
St Leonards NSW 2065

21 April 2023

Consumer Data Standards Australia
Treasury, Langton Cres
Parkes ACT 2600

Sent via email: contact@consumerdatastandards.gov.au

Noting Paper 296: Offline Customer Authentication

AGL Energy (AGL) welcomes the opportunity to provide feedback on Noting Paper 296: Offline Customer Authentication, published on 17 March 2023.

AGL is one of Australia's largest energy-led multi-service retailers, providing over 4.3 million electricity, gas and telco services to residential, small, and large businesses, and wholesale customers. AGL takes its privacy obligations and the security and protection of its customer data records extremely seriously.

AGL has reviewed the options for offline customer authentication put forward in the Consultation Paper and, at this stage of CDR implementation for energy retailers, we consider that it is most appropriate for the DSB to retain the current authentication framework for both offline and online customers until:

- The Federal Government finalises its large-scale review of the Privacy Act 1988[1], following which we anticipate that major data security reforms will come into effect. It is prudent to await the outcome of the review and to align the direction of CDR customer authentication requirements with the prospective Privacy Act changes to avoid duplicative effort or creating new offline authentication pathways which may be at risk of being redundant; and
- The expansion of CDR rules into the telecommunication sectors, which as we understand, could occur in 2023-2024. The DSB will be aware that the Australian Media and Communications Authority (ACMA) already imposes strict multi-factor identity authentication requirements (MFA) where a high-risk interaction is initiated between the customer and their telco service provider. Future customer authentication reforms should focus on establishing consistent authentication processes across sectors as this is the primary purpose of CDR and will help minimise costs for data holders across multiple designated CDR sectors.

We also note that the Consultation Paper proposes deprecating redirect with One Time Password (OTP) entirely, which we assume is intended to overcome any perceived inconvenience or barriers associated with authentication via the OTP which may be sent to another device. AGL does not support any model that ultimately weakens authentication requirements and the security of customers' personal information. Further, deprecation of the OTP for offline CDR users appears to be in conflict with ACMA's MFA requirements and contrary to the intention to heighten, rather than weaken, data security controls.

[1] Attorney-General's Department, Review of the Privacy Act 1988.

It is important to consider that irrespective of which offline customer authentication model is adopted, energy CDR participants will need to invest a substantial amount of time, effort, and resources to implement and maintain these new processes. In AGL's experience, there is no widespread evidence that our offline customers are disadvantaged in this regard, unable to access/share their CDR data using the current authentication channels or that this type of reform is strongly desired by customers. It is AGL's recommendation that the existing CDR authentication rules are retained, and this consultation deferred until the Privacy Act review recommendations and telco CDR designation come into effect.

Online and offline customer authentication

The Consultation Paper proposes creating a separate authentication pathway for offline customers which is distinct from the authentication requirements for online or digitally enabled customers. Tier 1 energy retailers have only recently invested significant financial and people resources to develop and deliver their current authentication solutions. There is limited data to substantiate that these solutions are not fit-for-purpose or are ineffective for the offline customer segment. Any changes to these processes will incur additional and unnecessary costs. The DSB should only propose changes to the CDR authentication process if there is clear evidence that offline consumers have found the current processes restrictive. No such evidence specific to the energy sector exists to support changes to recently implemented authentication processes.

From both cybersecurity and customer experience perspectives, there is limited merit in developing two separate verification and authentication pathways, and no indication that existing solutions are resulting in poorer customer outcomes. A fragmented approach between offline and online customers is more likely to result in an unsatisfactory customer experience, particularly for customers that forget or may not be aware that they are digitally registered and have an online identity.

Further development and design work to segment the processes between offline and online customers will impose significant costs for participants and divert resources from the next CDR phase preparations. AGL's preference at this time is to maintain the current arrangements and alignment between online and offline customer authentication requirements, regardless of the digital registration method. We believe this will facilitate a smooth and successful authentication experience for all customers.

Aligning CDR authentication standards with other industry reforms

There are two major reforms that the DSB must await finalisation of before making any changes to offline CDR authentication to ensure consistency with these reforms and to avoid further changes to authentication as the current offline proposal do not align with any changes to the Privacy Act and CDR designation of telecommunications.

1. Telecommunications and CDR designation

The multifactor authentication requirements set out under the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022 impose additional security standards for high-risk interactions. Following CDR implementation in the telco industry, all CDR-related interactions would be classified as high-risk interactions and trigger the MFA rules.

AGL's recommendation for future CDR energy authentication reforms is to align them with the telco requirements and, rather than setting prescriptive rules, allow retailers to retain discretion over the identity mechanisms that can be used to authenticate customers, such as the account number, email address,

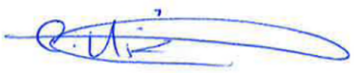
mobile number, etc. Further, as the telco MFA approach is flexible as to the account security information that can be accepted, it overcomes authentication issues in scenarios involving secondary account holders or authorised representatives that do not have an individualised account number, meaning that a bespoke solution for these customers segments is not required.

2. Privacy law review

Any future revision of authentication standards should also take into account the outcomes of the Privacy Act review. We caution against pursuing changes to the offline authentication process prematurely, particularly before the full scope of the Privacy Act review recommendations is known. Doing so may result in the design and development of multiple iterations of customer authentication standards, creating avoidable resourcing and financial pressures which would ultimately be worn by consumers.

If you would like to discuss any aspect of AGL's feedback, please contact Valeriya Kalpakidis at vkalpakidis@agl.com.au.

Yours sincerely,



Con Hristodoulidis

Senior Manager, Regulatory Strategy

AGL Energy