Data Standards Body

Consumer Experience and Technical Working Groups

Noting Paper 296: Offline Customer Authentication

Publish Date: Friday 17 March 2023
Feedback Conclusion Date: Monday 17 April 2023
Contacts:
Bikram Khadka, Consumer Experience Designer
Holly McKee, Consumer Experience Designer
Michael Palmyre, Consumer Experience Lead

Overview

This query was originally posted as a comment on Noting Paper 280 as it relates to the CX (consumer experience) of authentication uplift. It has been separated out into its own Noting Paper for formal consultation following community requests to do so.

The purpose of this paper is to seek community feedback on offline customer authentication. The paper focuses on the impacts and opportunities regarding the augmentation or deprecation of the redirect with OTP (One Time Password) model.

The redirect with OTP' model allows a range of CDR (Consumer Data Right) consumers to authenticate to share CDR data. This includes 'offline customers', who are defined as consumers who do not currently have an online account with their data holder. Offline customers are currently only eligible in the energy sector.

As this article outlines, (energy) data holders must not impose additional eligibility requirements, such as requiring an offline customer to register for online account access before they can share data. That is, an offline customer must be able to authenticate to share CDR data using permissible details - such as a unique ID and contact information - already held by the data holder.

This approach means that a consumer without an online account could, for example, use an existing non-digital credential - like an account number - and have an OTP sent to them using contact details already held by the data holder, like an SMS or via email.

Similar scenarios may arise where customers are technically 'eligible' even though they lack an online account with the data holder. The recently published guidance from ACCC on Eligibility Across DH Brands suggests this may occur for multi-banked consumers, but it may also be possible in theory for accounts with multiple parties, such as secondary users, partnerships, joint accounts, and the nominated representatives of non-individuals (particularly in the energy sector).

The problem

Deprecation of the redirect with OTP model has been recommended to support CDR security and authentication uplift (see NP280 and NP258). Adopting this approach may have implications for offline customers and a range of energy retailers. Assumptions to be tested include:

- A significant proportion of energy consumers may be 'offline customers'. Based on limited data from major and non-major retailers in 2020:
    - an average of 73% of SME customers were offline, which was projected to reduce to 58.5% in 2021
    - an average of 49% of residential customers were offline, which was projected to reduce to 40% in 2021
- As such, deprecating the redirect w/ OTP model will effectively 'switch off' support for a non-trivial amount of CDR consumers who are currently eligible as per the rules and able to share CDR data today
- Some energy DHs may not provide online portals at all, meaning all of their customers are 'offline customers'
- Energy retailers mandated to share CDR data have been implementing CDR even if a significant proportion of, and in some cases all of, their customers are offline customers (which may apply to DHs in other sectors for certain scenarios described above)

Alternatively, risks and limitations of the OTP model for offline customers are assumed to include:

- Delivery of an OTP to an unverified contact detail, such as a mobile or email, which may be further complicated by lower levels of identity proofing for energy customers compared to banking
- This is further complicated by the low level of identity proofing for energy customers
- "Unique IDs" that may not be unique to the offline customer
- Single-factor OTP does not currently meet the assumed data sensitivity requirements for CDR data sharing. At present, the current authentication requirements for offline customers map to Credential Level 1 (CL1) as defined by the Data Transformation Agency's (DTA) Trusted Digital Identity Framework (TDIF). TDIF states that CL1 must only be used where risk of compromise will result in "negligible to minor consequences to the Individual or the service".
- Additional stronger security measures for offline customers are limited without a registered digital identity

Working hypotheses

The current hypothesis is that the redirect with OTP model may be a critical fallback option for less digitally mature sectors, as well as for offline customers. However, recommendations have been made for redirect with OTP to meet CL1-2, if not be deprecated entirely, which may preclude the ability for offline customers to be authenticated.

For customers with online accounts, achieving CL2 using redirect with OTP may be possible. For offline customers without online accounts, CL1 may be possible. If CL3 is required for action-initiation, it is unlikely that offline customers will be able to participate.

Questions for consultation

The DSB is seeking community input on the risks, trade-offs, and implications of:

- retaining the current redirect with OTP for offline customers; or
- deprecating redirect with OTP entirely; or
- requiring that the redirect with OTP model meet a higher credential level (e.g. CL1, CL2); or
- pursuing an alternative to maintain support for offline customers

Community input should consider security risks, consumer experience, as well as the costs and implications for DHs, particularly in energy, who have been, or are in the process of, implementing the current model to support authentication for offline customers. It should also consider the potential need to continue supporting offline customers for future sectors that have low levels of digital adoption.

The following questions may be used to guide submissions:

1. How might we augment the redirect w/ OTP flow/mechanism to maintain support for offline customers?
2. If it is not appropriate to retain the redirect w/ OTP flow at all, what alternatives exist to maintain support for offline customers?