

BASIQ

Transitioning to Open Banking

HOW TO PREPARE IN USING OPEN BANKING

What you need to know

As more financial institutions share data via Open Banking, make sure you're ready for the transition and have considered the following 5 steps to prepare yourself.

01 User Experience - What are the UX guidelines for Open Banking?

- Customer consent underpins the CDR, so the communication of consent along the customer journey is critical. Did you know there are 5 different types of consent that you may need to request from your customers?
 - **Collection Consent:** What data do you want to collect
 - **Use Consent:** Why you need to collect it (primary use)
 - **Disclosure Consent:** Sharing it with 3rd parties
 - **Direct Marketing Consent:** a form of 'use consent' where it is used for direct marketing purposes
 - **De-Identification Consent:** a form of 'use consent' where data is de-identified for research and disclosure (including selling)

02 Data Governance - What are the rules in holding and managing CDR data?

- The CDR regime places the value and control of the consumer data in the hands of the consumer
- There are strict requirements on data governance in relation to the collection, use and disclosure of CDR data for ADRs
 - Collection of consent Purpose
 - Collection of consent time period
 - Provision of a consumer dashboard
 - Consumer notifications of consent changes
 - Ongoing notification requirements

03 Security - What are the required security standards?

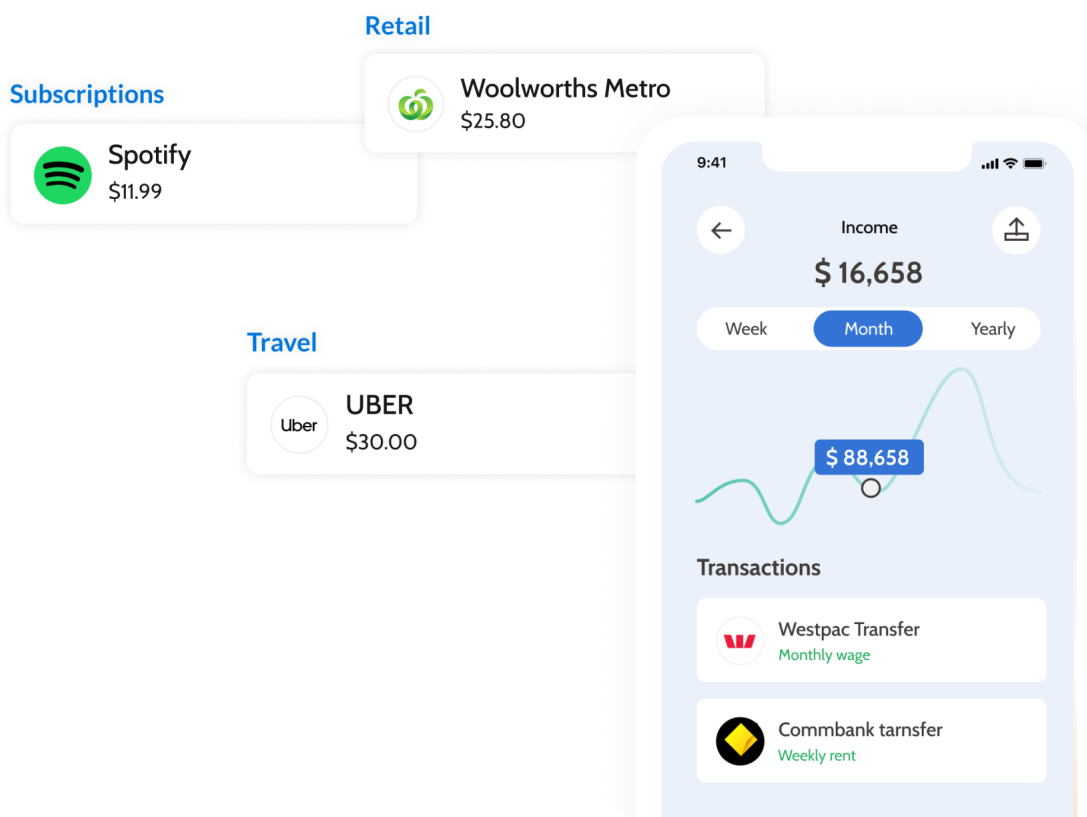
- The CDR sets out specific requirements on the level of security you need in order to be able to use Open Banking data and consists of two parts.
 - **Documentation:** The CDR environment must be assessed, defined, documented and periodically reviewed in relation to:
 - Organisation & people
 - Processes
 - Technology security platform
 - **Controls:** Controls are in place for the CDR data environment in relation to:
 - Data access
 - Security of network and systems
 - Security of information assets
 - Vulnerability management program
 - Preventing, detecting & removing malware
 - Information security training

04 Data Coverage - Will I get sufficient coverage via Open Banking data?

- The CDR Regime only requires Australian Deposit Taking Institutions (ADIs) to share data via Open Banking with Non-Bank Lenders soon to join
- There may be instances where data from non-ADI financial institutions is important for your business
- Not all ADIs are currently sharing financial data via Open Banking and there are many exemptions currently in place
- Consideration of complementary methods of data access alongside Open Banking may be beneficial

05 Accreditation - What approach should I take in becoming accredited?

- In order to participate in using Open Banking, organisations are required to be accredited by the ACCC and become an Accredited Data Recipient (ADR)
- These new pathways include Sponsored Affiliate, Principal and Representative, Trusted Advisor and CDR Insights
- The ACCC has also created a number of new pathways with unrestricted access to Open Banking where organisations can leverage the use of an ADR.
- While Outsourced Service Provider are not an access model, an ADR (the Principal) can engage an OSP to collect CDR data on their behalf or provide goods and services using the CDR data it has collected.



Your checklist

There are some areas you can take action on **TODAY** to ensure you're ready when the CDR is nearing the end of its rollout. Use the checklist below to begin preparing for your transition to using Open Banking data.

01 User Experience

- Review the [CX Guidelines](#) as a reference of how consent flows may need to work for your business
- Implement a consent capture screen that takes into account the consent use types you intend to use for Open Banking and perform A/B testing ahead of time to optimise your UI & UX

02 Data Governance

Start thinking about different consent types that apply to your use case and how you will apply them to the data you hold

- Ensure consent data is captured and managed within the CDR consent framework
- Ensure Consents are valid for no longer than 12 months
- Ensure data can be anonymised and can be “deleted” at the consumer’s request
- Develop best practice and ensure data is only used for the purposes upon which it was requested and consented for
- Develop and communicate a policy of how redundant data is treated

03 Security

- Outline the security of CDR data and destruction or de-identification of redundant CDR data
- Define and implement security governance in relation to CDR data
- Define the boundaries of the CDR data environment
- Have and maintain an information security capability
- Implement a formal controls assessment program
- Manage and report security incidents

04 Data Coverage

- Review who is currently sharing data via Open Banking [here](#), to determine if Open Banking provides you with requisite coverage
- If not, Consider using a complementary approach to Open Banking for those that are not currently sharing data to optimise coverage.
- Basiq is able to provide a combination of Web Connections and Open Banking data, through our dynamic switching capability, to ensure you have optimal coverage until more financial institutions are part for the CDR regime.

05 CDR Accreditation

- Review the different access models to determine the most optimal pathway for your organisation. These include:

1: Principal Representative Model (PRM)

There is no official accreditation needed, instead a business is able to access data as a Representative via an ADR that acts as a Principal.

2: Sponsored Affiliate (SM)

Businesses who become a Sponsored Affiliate have accredited access to data via an ADR acting as a Sponsor. This model allows Sponsored Affiliates some of the same privileges and access to CDR data as an ADR, but at a lower cost and in less time.

3: Outsourced Service Provider (OSP)

While this is not a CDR access model, an ADR (the Principal) can engage an OSP to collect CDR data on their behalf or provide goods and services using the CDR data it has collected.

4: Trusted Advisor (TA)

This model allows consumer consented data to be shared with 'trusted advisors', including financial advisers, mortgage brokers, accountants, tax agents and/or lawyers.

5: CDR Insights

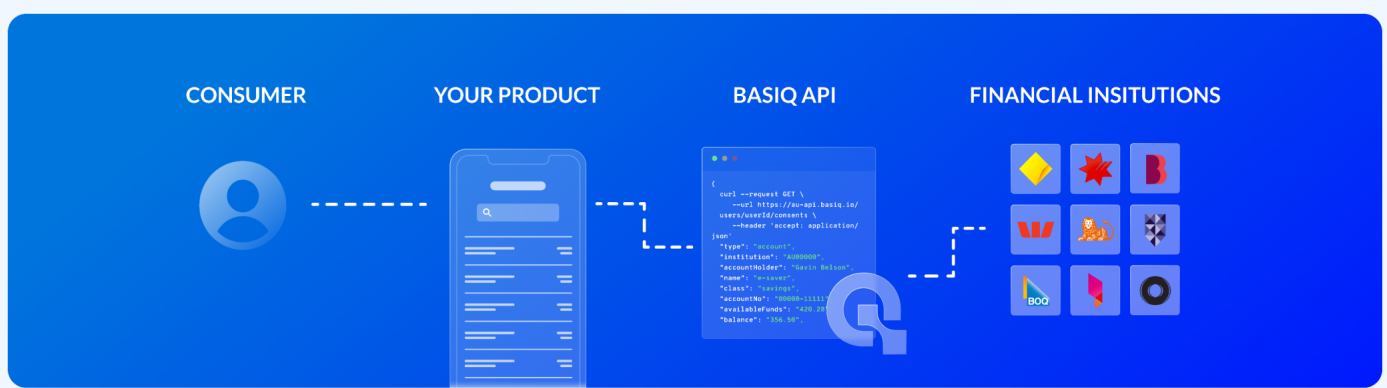
CDR rules allow consumers to share insights with individuals or organisations outside the CDR ecosystem for specific low-risk purposes, including verifying a consumer's identity, account balance, or details of transactions to or from specified accounts.

- [Click here](#) to review the different CDR access models

Basiq is an API platform that provides the building blocks of financial services

At Basiq, our vision is Making Finance Easy. Finance is complex and it can be hard for consumers to make informed financial decisions. We see a world where consumers are empowered to make smarter financial decisions and to engage with their finances in new and unique ways.

Basiq enables this by providing an Open Finance API platform for businesses to build innovative financial solutions. The platform facilitates the relationship between financial fintechs and consumers by enabling access to consented financial data and providing payments services.



Why partner with us



Knowledge & Expertise

Years of experience in accessing and driving insights from financial data through RESTFUL and fully documented APIs.



Scalability & Reliability

Helped over 2.5m consumers share their data on the platform with over 1m data requests per day.



Open Banking provider

Recognised as a provider of Open Banking services by the ACCC as an Accredited Data Recipient under the CDR.



Developer Tooling

Accelerate development with Basiq's developer starter kits, best practice quick start guides and API documentation.



Single Platform

A single integration to plug in to the Basiq platform to access data, insights and payments services.



Local Support

A dedicated local support team that ensures smooth implementation, continuous support and fast response times.



BASIQ

basiq.io

The material in this information resource is being used for marketing and/or promotional purposes only. While we make efforts to ensure accuracy, we cannot guarantee the completeness or reliability of the information contained within. We also do not provide guarantees in respect of any products, services, or external sources referenced within. Your use of the material is at your own discretion and risk. We disclaim all liability for any loss or damage resulting from its use. This information resource and the content within it is protected by copyright and trademark laws. This disclaimer may be updated at any time, and your continued use of this material indicates your acceptance of the terms.