OPEN BANKING AND THE CUSTOMER EXPERIENCE

Produced by FUTURE OF PRIVACY FORUM FPF.ORG

Open banking via APIs allows companies to access customer data to provide new products and services. It can enable less costly, more inclusive, higher quality services, while increasing convenience, speed, and competition. However, the state of open banking in the United States can create challenges for customers wishing to use these services. Let's take a look...

CUSTOMER
Individuals who want a digital financial service.

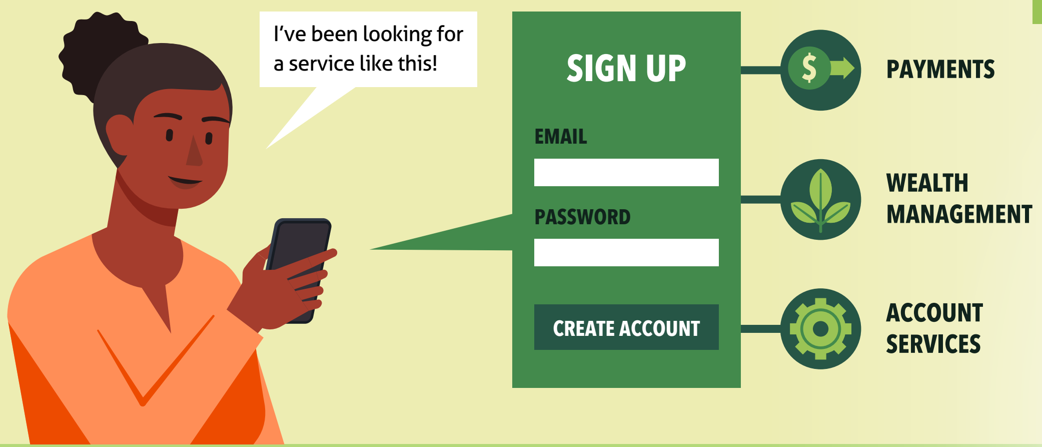
DATA RECIPIENTS
Companies that need customer data to provide requested services.

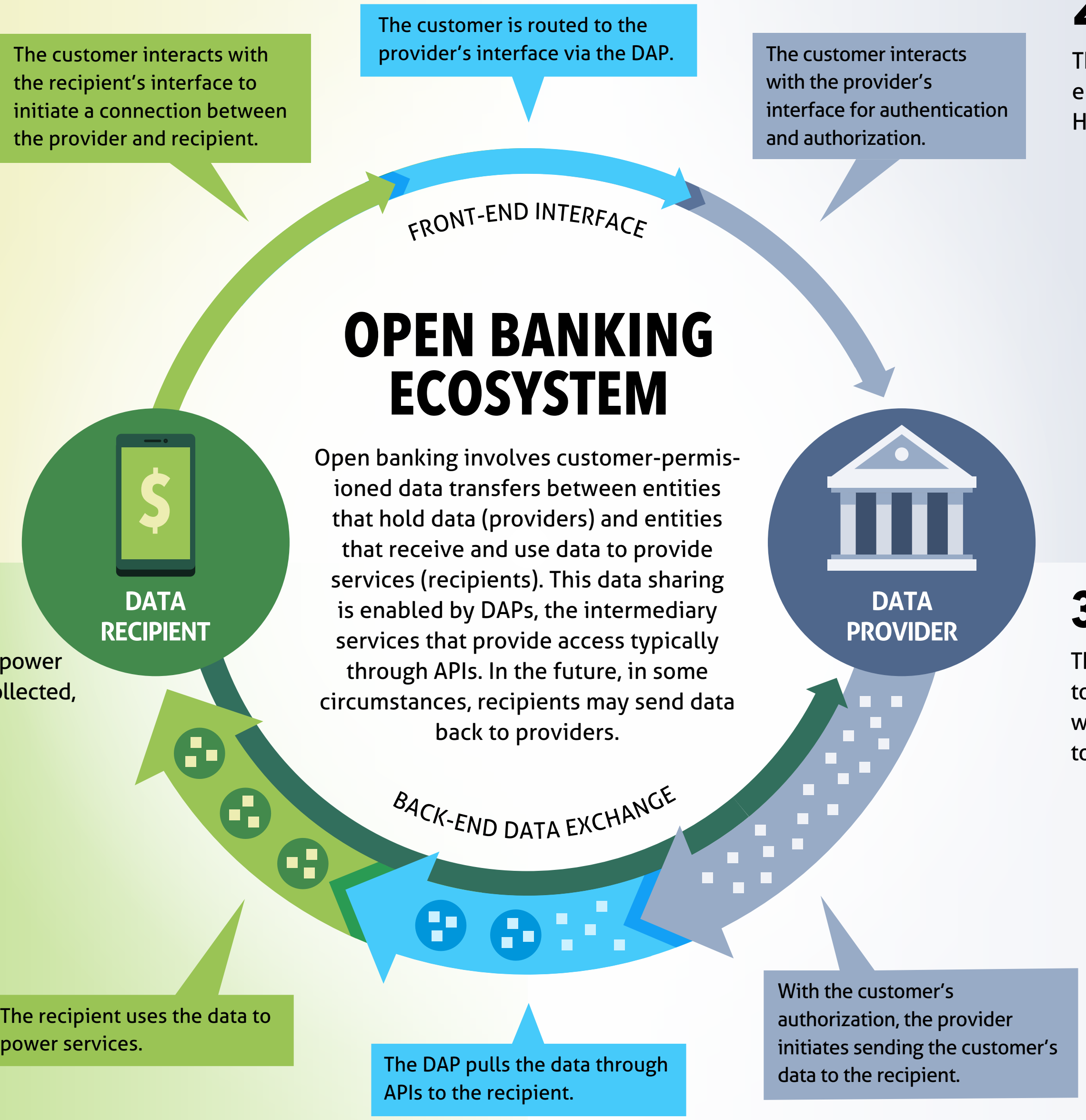
DATA ACCESS PLATFORMS (DAP)
Intermediaries that support data flows between data recipients and data providers.

DATA PROVIDERS
Companies like banks or card issuers that hold customer financial data.

1. SIGN UP & INITIATE SERVICE

The customer requests that a company provide a service such as online payments, wealth management tools, or account information services.





Open banking involves customer-permissioned data transfers between entities that hold data (providers) and entities that receive and use data to provide services (recipients). This data sharing is enabled by DAPs, the intermediary services that provide access typically through APIs. In the future, in some circumstances, recipients may send data back to providers.

The customer interacts with the recipient's interface to initiate a connection between the provider and recipient.

The customer is routed to the provider's interface via the DAP.

The customer interacts with the provider's interface for authentication and authorization.

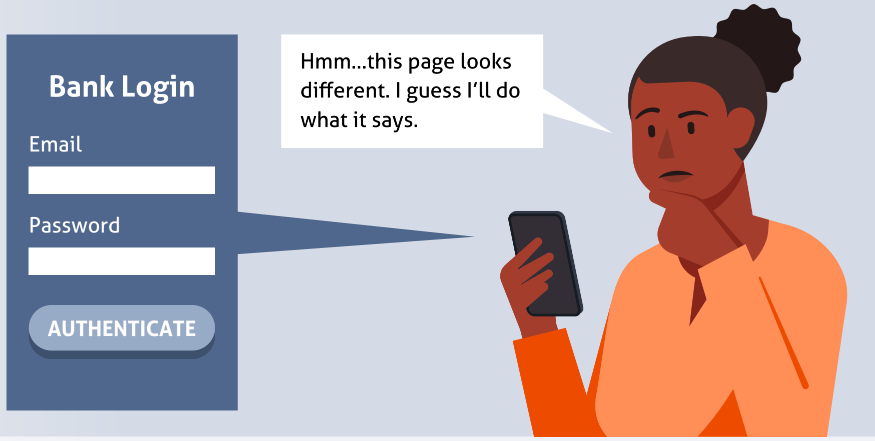
With the customer's authorization, the provider initiates sending the customer's data to the recipient.

The DAP pulls the data through APIs to the recipient.

The recipient uses the data to power services.

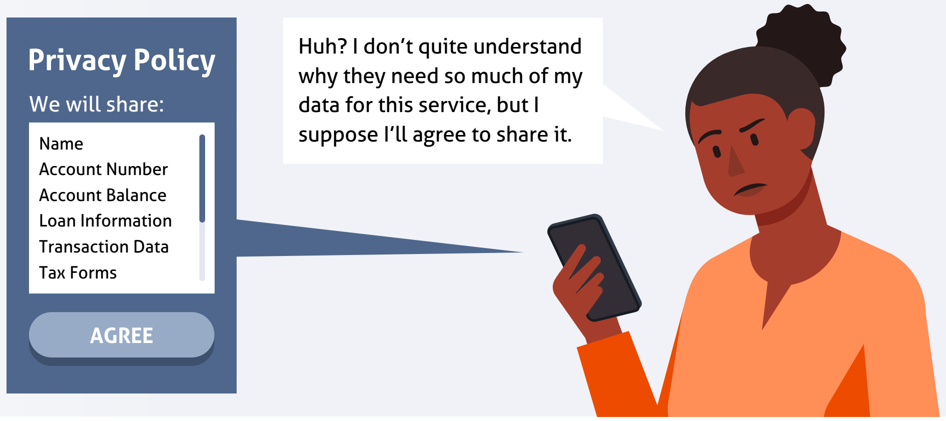
2. AUTHENTICATE IDENTITY

The customer may be redirected to the data provider to authenticate their identity. Businesses employ many authentication methods. Often, customers navigate these windows with ease. However, confusing user interfaces may deter some customers.


Bank Login
Email
Password
AUTHENTICATE
Hmm...this page looks different. I guess I'll do what it says.

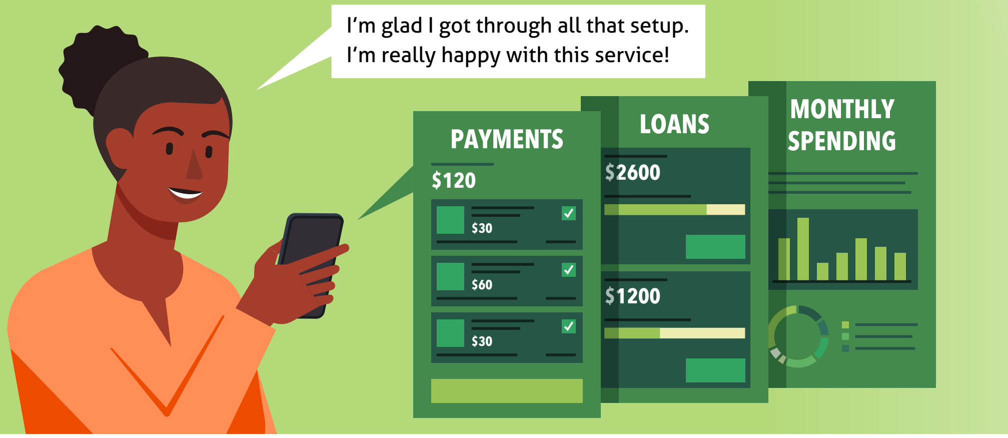
3. AUTHORIZE DATA SHARING

The customer authorizes the data provider to send data to the recipient. The customer sees options to share certain types of information. Providers won't know exactly how the data will be used or why it's necessary for the data recipient's service. Providers, recipients, and DAPs must work together to ensure the customer stays informed.


Privacy Policy
We will share:
Name
Account Number
Account Balance
Loan Information
Transaction Data
Tax Forms
AGREE
Huh? I don't quite understand why they need so much of my data for this service, but I suppose I'll agree to share it.

4. PROVIDE SERVICE

The recipient uses the data to provide the requested service to the customer. Open banking can empower customers but must be easy to use and understand. Stakeholders should clarify what data will be collected, to whom it will be shared, how it will be used, and should get consent for any secondary uses.


I'm glad I got through all that setup. I'm really happy with this service!
PAYMENTS
$120
$30
$60
$30
LOANS
$2600
$1200
MONTHLY SPENDING

PAIN POINTS

NOTICE AND CONSENT
Current rules do not address many issues about which parties provide notice and collect consent, or about which activities require consent. This leads to inconsistency, over or under data collection, and less transparency about uses.

ROLES AND RESPONSIBILITIES OF PARTIES
Open banking involves multiple parties. However, these parties' roles and responsibilities remain unclear, creating uncertainties and friction. Coordination by appropriate regulators could help reduce uncertainty and prevent inconsistent oversight mechanisms and rules.

SECONDARY DATA USES
Customers may be surprised by how parties use their data beyond the original (primary) purpose. These secondary uses pose customer risks given the sensitivity of financial data. Rules should require consent for secondary uses.

DATA RETENTION
Customers may expect their data to be deleted upon request or when the service ends. Conversely, companies often have legal obligations to keep data. Regulators should consider rules for retention and deletion, which are currently unclear.

CUSTOMER SERVICE AND TERMINATIONS
Without clear roles and responsibilities, customers may not know who to consult to fix issues. It is unclear how parties should communicate changes with one another, or when to cease use of customers' data.