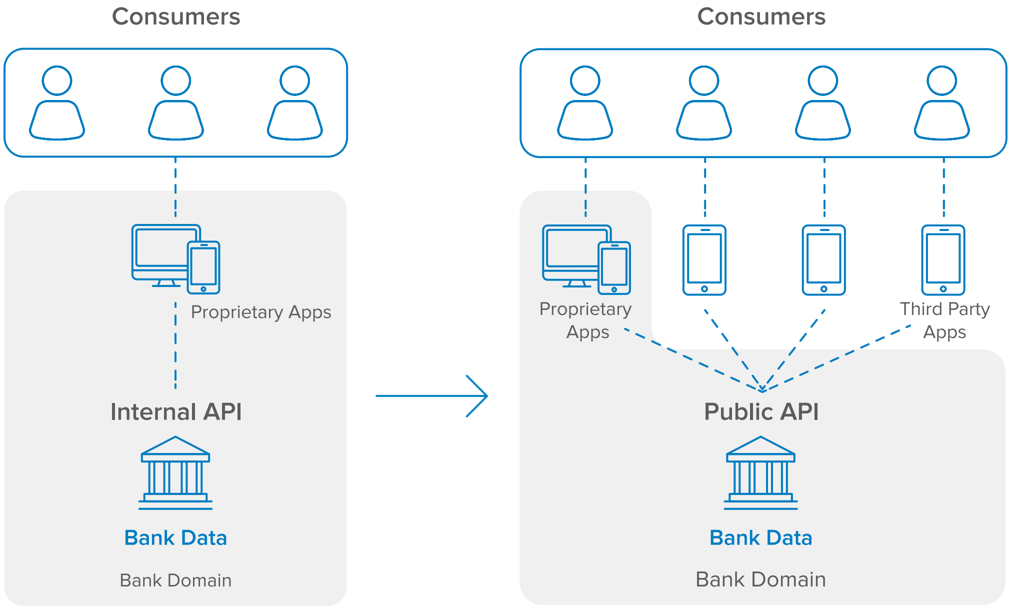
Implications Around PSD2 and Open Banking

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

What Is PSD2 and Open Banking?

Traditionally, banks and other financial institutions have held a monopoly over their customer's account information and payment services. Many of these financial institutions have invested in digital innovation to provide modern experiences via their websites and mobile applications. However, for the most part, consumers don't have a choice in how they can access their banking services. In contrast, if we look at email as an example, consumers have the flexibility to use their preferred client to read and send mail, such as browser clients (e.g. mail.google.com), email software (e.g. Microsoft Outlook or Thunderbird), or Native OS clients (e.g. IOS), regardless of which email service provider they are using (e.g. Gmail, Yahoo Mail, etc.). PSD2 and Open Banking aim to facilitate this exact paradigm shift in banking.



The second payment services directive, or PSD2, is a European Union regulation that requires all European banks to expose their customer account data to allow third parties to manage their finances through open APIs (application programming interfaces). Banks and other financial service providers must also comply to specific security measures outlined in the Regulatory Technical Standards (RTS). PSD2 took effect on January 13, 2018, with the exception of the security measures outlined in the RTS, of which companies have 18 months (up until July 13, 2019) to implement.

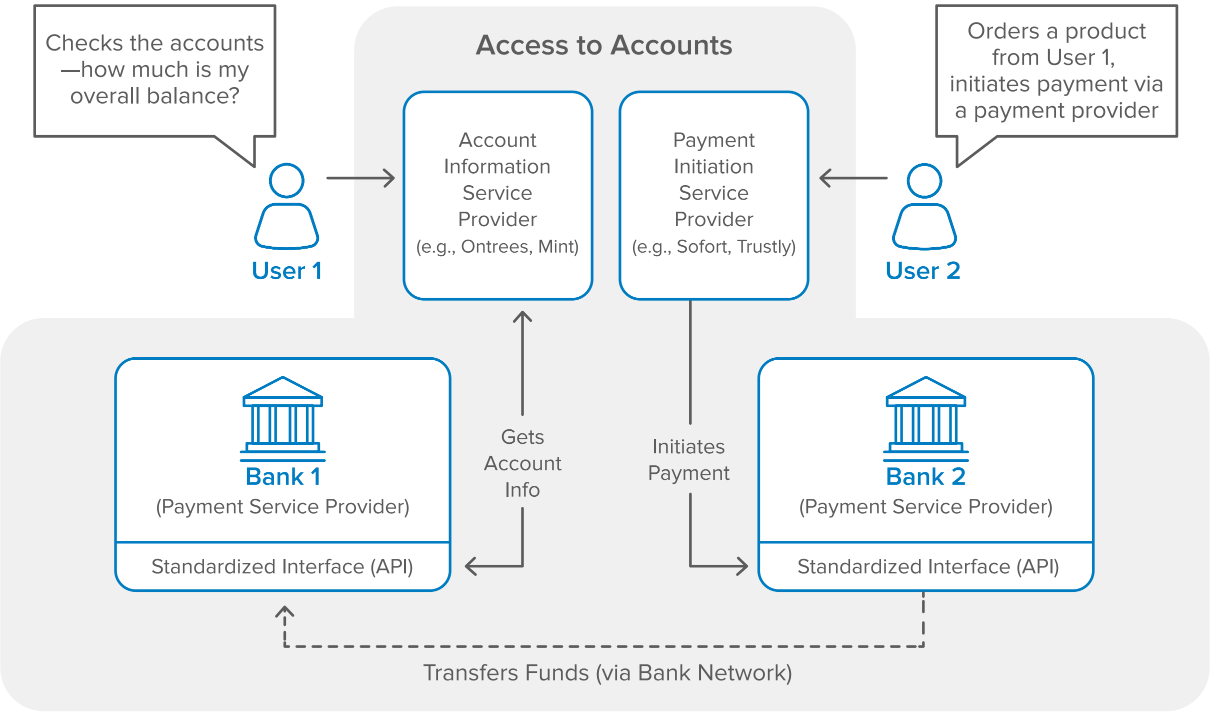
Following in the EU's footsteps, the United Kingdom and Australia have also enacted their localized version of an Open Banking regulation which mandates similar requirements for financial institutions to provide third-party access to customer account data with secure and open APIs. UK's Open Banking initiative took effect on January 13, 2018, aligning with PSD2. Australia's Open Banking will enforce a deadline of July 1, 2019, for the four major banks to comply, and then an additional 12 months (up until July 1, 2020) for all of the remaining financial institutions to comply.

The rest of the world is paying close attention. Although many countries have not passed official legislation mandating Open Banking, financial institutions around the globe are actively preparing by modernizing their digital platforms to provide secure API access to share customer data.

Who Are the New Players?

PSD2 and Open Banking will open up the market to new entrants to give consumers more flexibility and choice on how to manage and spend their money. For example, in the United States, financial account aggregator Mint.com paved the way as the first widely adopted Account Information Service Provider (AISP). Similarly, Intuit's TurboTax added the ability to directly import tax statements from financial institutions, significantly simplifying the process of populating income and loss sources into tax forms. However, it is important to note that both of these examples are using unsecure methods where consumers are directly passing their credentials to the AISP to log into their financial services accounts on their behalf and using methods such as screen scraping to fetch data.

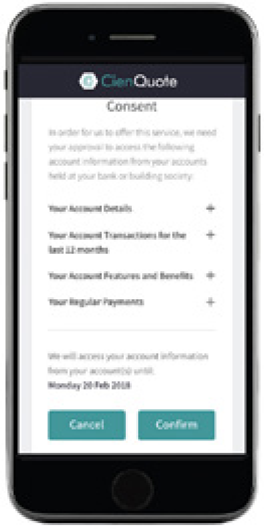
Additionally, Payment Initiation Service Providers (PISPs) such as Sofort, Trustly, and Swish allow consumers to instruct their banks to initiate payments via APIs. PISPs are different than existing payment services such as Stripe or Apple Pay where banks still review and approve every transaction. The real-time speed of these transactions is an advantage in peer-to-peer transfers or ecommerce use cases, but also creates new security concerns—in particular around authenticating higher risk transactions. Note, as of now, Australia's Open Banking regulations only mandate banks to expose read access, limiting the ability for third-party applications to initiate payments (which requires write access).


Checks the accounts —how much is my overall balance?
Access to Accounts
Orders a product from User 1, initiates payment via a payment provider
User 1
Account Information Service Provider (e.g., Ontrees, Mint)
Payment Initiation Service Provider (e.g., Sofort, Trustly)
User 2
Bank 1
(Payment Service Provider)
Standardized Interface (API)
Gets Account Info
Initiates Payment
Bank 2
(Payment Service Provider)
Standardized Interface (API)
Transfers Funds (via Bank Network)

As PSD2 and Open Banking forces banks and financial institutions to open up APIs, consumers should expect far more AISP and PISP options to be available to them, creating a whole new playing field. Banks will have to decide whether they want to be relegated to a "utility" or act as a verticalized service provider, in which they will continue to own the end user relationship with their customers via their web and mobile applications.

What Are the Technical Requirements?

PSD2, Open Banking (UK), and Open Banking (Australia) dictate unique technical requirements, but also share some core components. All of these standards mandate a 3-legged consent flow, which will be described here. First, a third-party application must request explicit consent from users to initiate payments or access data from their financial institution. Next, users will be redirected to the financial institution to be authenticated. Once the user's identity is verified, the financial institution will then present a list of requested permissions that the third-party application is asking for back to the user, which they must confirm to authorize access. Finally, users will be redirected back to the third-party application to proceed with their desired action.



CienQuote

Consent

In order for us to offer this service, we need your approval to access the following account information from your accounts held at your bank or building society.

Your Account Details +

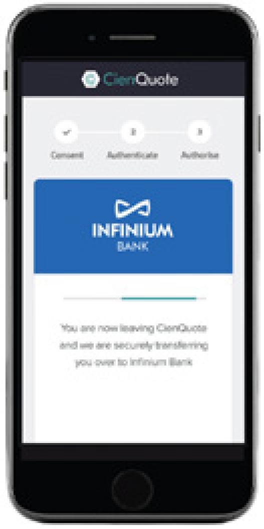
Your Account Transactions for the last 12 months +

Your Account Features and Benefits +

Your Regular Payments +

We will access your account information from your account(s) until: Monday 20 Feb 2018

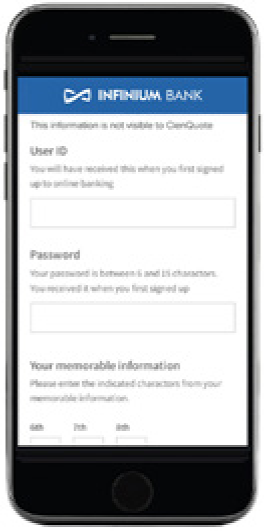
Step 1: Consent



CienQuote

You are now leaving CienQuote and we are securely transferring you over to Infinium Bank

Step 2: Redirect to Financial Institution



INFINIUM BANK

This information is not visible to CienQuote

User ID

You will have received this when you first signed up to online banking

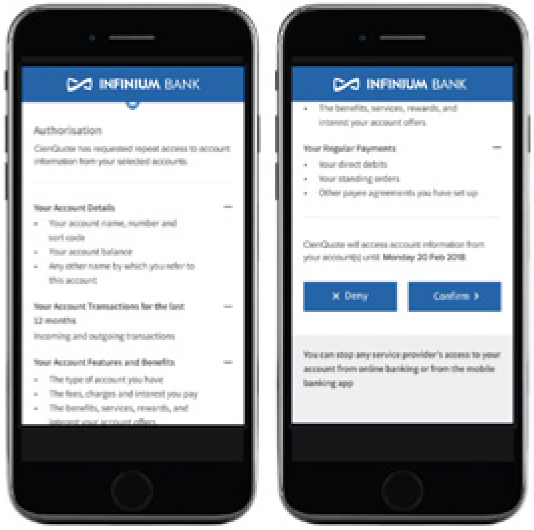
Password

Your password is between 6 and 15 characters. You received it when you first signed up

Your memorable information

Please enter the indicated characters from your memorable information

Step 3: Authenticate User



INFINIUM BANK

Authorisation

CienQuote has requested repeat access to account information from your selected accounts

Your Account Details –
- Your account name, number and sort code
- Your account balance
- Any other name by which you refer to this account

Your Account Transactions for the last 12 months –

Incoming and outgoing transactions

Your Account Features and Benefits –
- The type of account you have
- The fees, charges and interest you pay
- The benefits, services, rewards, and interest your account offers

INFINIUM BANK

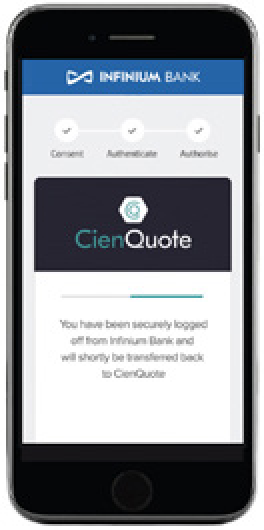
- The benefits, services, rewards, and interest your account offers

Your Regular Payments –
- Your direct debits
- Your standing orders
- Other payee agreements you have set up

CienQuote will access account information from your account(s) until: Monday 20 Feb 2018

You can stop any service provider's access to your account from online banking or from the mobile banking app

Step 4: Authorization and Confirmation



INFINIUM BANK

You have been securely logged off from Infinium Bank and will shortly be transferred back to CienQuote

Step 5: Redirect Back to Third-Party Application

In order to ensure secure access to extremely sensitive and personal data, PSD2 and Open Banking mandates that all parties involved leverage financial-grade API (FAPI) security defined by the OpenID Foundation working group, which is also responsible for maintaining the OpenID Connect (OIDC) standard protocol built on top of OAuth 2.0 that is used for identity and access management (IAM). In addition to requiring OIDC/OAuth 2.0 as the mechanism for authentication and authorization, FAPI dictates specific technical requirements such as compliance to TLS 1.2 as defined in [RFC5246] with usage following the best practice in [RFC7525], as well as the capability for end users to revoke or refresh authorization via access tokens as defined in [RFC7519].

Additionally, for PISPs to initiate payment transactions, PSD2's Regulatory Technical Standards has defined a strict set of requirements for authentication known as Strong Customer Authentication (SCA). By September 14, 2019, all payments that are initiated by customers and exceeding €30 will require authentication using at least 2 out of the following 3 elements:

1. Something that only the customer knows (i.e. password, PIN, security question)
2. Something that only the customer possesses (i.e. hardware token, mobile phone)
3. Something that the customer is (i.e. biometrics, detection of unique behavioral patterns)

The amount of the transaction and the business being paid must be explicitly confirmed by consumers. PISPs and financial institutions will also be held responsible to monitor and detect unauthorized or fraudulent payments.

How Can Okta Help?

Okta **API Access Management** can help banks and financial institutions comply with PSD2 and Open Banking's requirement to expose sensitive consumer data via APIs in a secure manner. Financial institutions can create and customize a user consent page that is hosted by Okta and served to downstream 3rd-party apps. Okta's API Access Management also integrates with popular API Gateways, including Apigee, Mulesoft, Amazon API GW, Azure API GW, SoftwareAg, Kong, and Tyk, allowing flexibility and choice of platform.

Okta **Customer Identity solutions** provides a digital identity layer for banks, financial institutions, AISPs, PISPs, and other application developers to create seamless and secure experiences. Okta provides out-of-the-box components such as **Self-Service Registration** and the **Okta Sign-in Widget** to easily embed common use cases such as user registration and authentication flows, significantly speeding up application development and reducing costs.

Okta **Adaptive Multi-factor Authentication (AMFA)** protects your users against account takeover while minimizing user friction. Okta AMFA allows for dynamic policy changes and step-up authentication in response to changes in user behavior, location, use of new/untrusted devices, or other contexts.

Okta supports a wide range of authentication factors that meet the PSD2 Strong Customer Authentication requirements for payment transactions including:

- SMS, voice, and email
- Security questions
- Time limited one-time passwords
- Push notifications to Okta Verify or other 3rd-party solutions
- Device fingerprinting
- Physical tokens
- Biometrics-based factors such as Apple Touch / Face ID

For more information on how Okta can help with your PSD2 and Open Banking initiatives, please visit:

https://www.okta.com/psd2-and-open-banking/

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,000 applications, the Okta Identity Cloud enables simple and secure access for any user from any device.

Thousands of customers, including 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn, and News Corp, trust Okta to help them work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

Learn more at: www.okta.com

okta