Solution Brief
May 2021

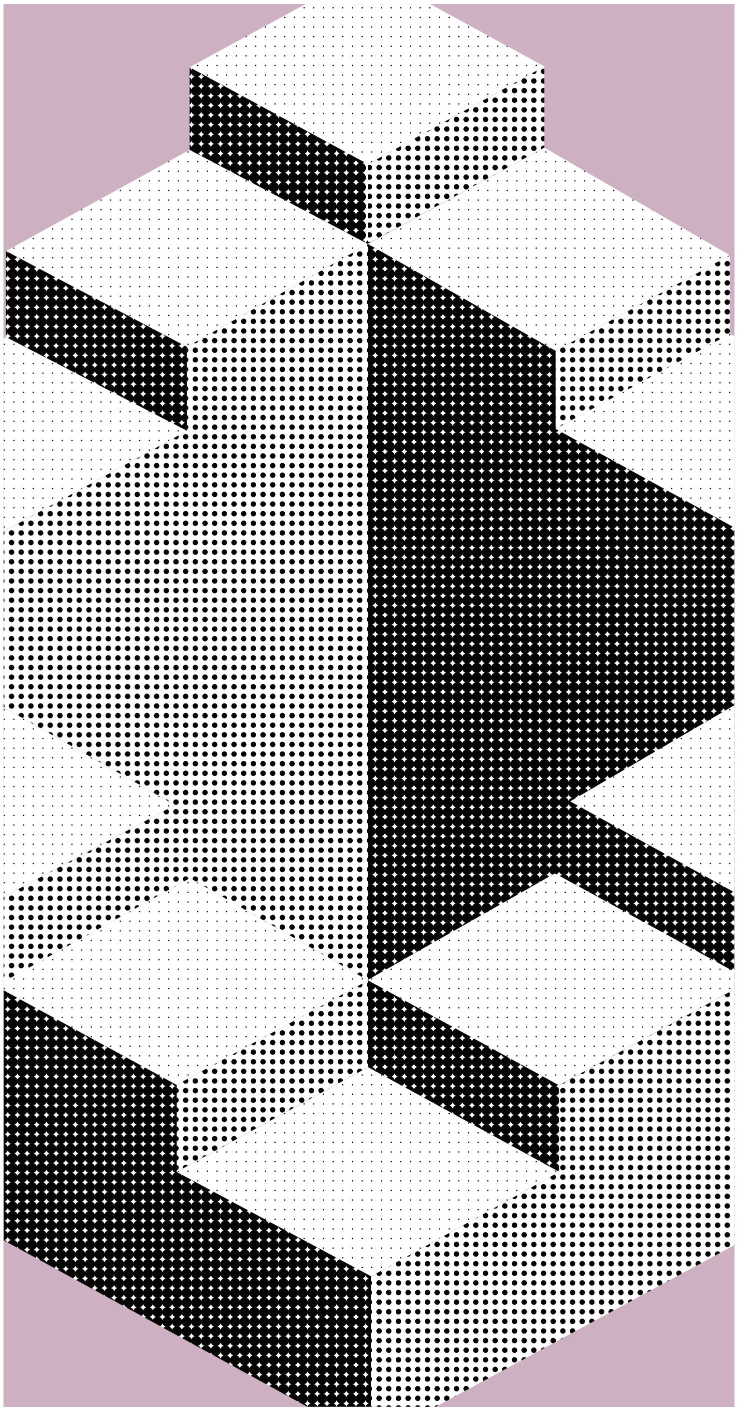
Okta + Cloudentity: Embrace Open Banking And PSD2 Compliance

Accelerating digital transformation is nothing new for financial institutions. Regulatory changes have always been key drivers of reshaping the financial services industry, through expediting modern technologies and services to provide better products, services and privacy for bank customers.

Most recently, Open Banking protocol—designed to spur customer-first innovation in financial services—has been sweeping the world, ever since the European Union's 2018 adoption of the revised Directive on Payment Services (PSD2). Inspired, countries around the world have adopted best practices from Europe's PSD2, including CDR in Australia, Open Banking in the UK, Canada, Nigeria, Australia, and Brazil, and the Financial Data Exchange (FDX) in the US.

But the consumer-friendly changes proposed by Open Banking standards pose significant technical and procedural challenges.

The Okta + Cloudentity joint solution can help financial institutions adjust to their new responsibilities and safely innovate customer experiences, now and on an ongoing basis.



okta | CLOUDENTITY

What is PSD2?

PSD2 is an amendment to the 2007 Payment Service Providers Directive, a European Union initiative originally designed to support an efficient single payment market. PSD2 takes that initiative further, spelling out specific requirements to protect consumers, increase security, and spur innovation in the financial services sector.

PSD2 is designed to support three important principles:

- **Empower** and protect customers with consumer consent
- **Secure** payments with strong customer authentication for transactions
- **Promote** innovative services and products through the Open Banking concept

What is Open Banking?

Open banking is the practice of sharing customer financial information electronically, securely, and only under conditions that customers approve of. This customer-centric ecosystem uses secure APIs to share consumer data—with customer consent—between banks and third-party providers.

Open Banking permits all kinds of innovations for customer financial services, including the following:

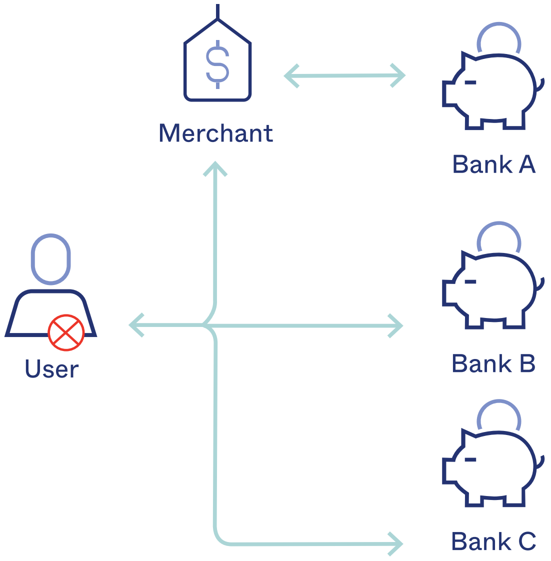
- **Build** customer privacy and comprehensive consent into all data sharing of personally identifiable information (PII)
- **Protect** consumer data in transit via FAPI, the gold standard for API protection
- **Provide** customer-centric flows for ease of use and integrations between banks and third party financial services providers

Open Banking: New Privileges, New Responsibilities

With Open Banking, financial institutions are broadly required to grant third-party providers (such as emerging FinTech companies) secure access to customer accounts, via a direct connection known as an XS2A API. This Open Banking API, governed by fine-grained consent management, authorizes API-driven access to otherwise private account and transaction information like payment initiation.

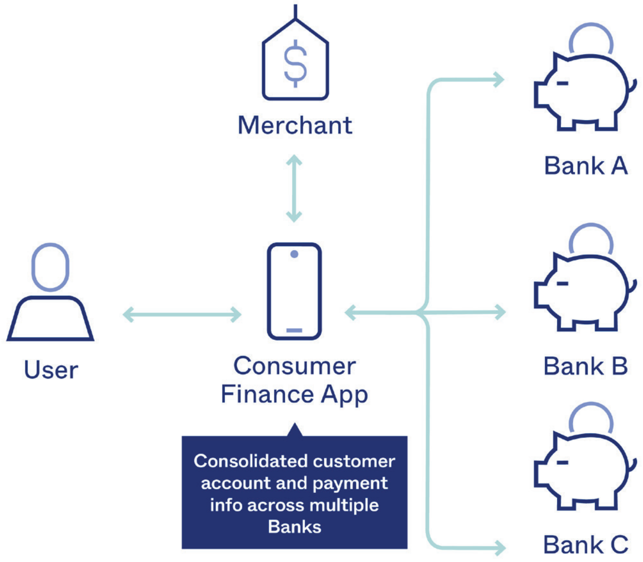
The promise of Open Banking is that it gives customers better experiences and better control over their data. But for financial institutions, the Open Banking standard also imposes new burdens. It can be complicated and expensive to implement, and opening a bank's application programming interfaces (APIs) to third-party providers entails significant security risks. These include the potential for data loss, identity theft, account takeovers, data protection violations, money laundering and a host of specific API risks summarized in the OWASP API Top 10.

Open Banking is designed to usher in an age of innovation, giving banking consumers easier and better ways to manage their personal data, financial wellness and payment transactions, and around the world, financial institutions are feeling the pressure to quickly move into compliance. They need a strategy for carrying out large-scale innovation of the customer experience without jeopardizing security and customer trust. For many financial institutions it boils down to choosing simple compliance, by partnering with a faster-moving FinTech company that can move them quickly into compliance, or investing in developing these technologies themselves.



Before PSD2 and Open Banking

Transaction-focused, designed to benefit banks and merchants; customer has disconnected and frustrating experiences


Merchant
Bank A
User
Consumer Finance App
Bank B
Consolidated customer account and payment info across multiple Banks
Bank C

With PSD2 and Open Banking

Consumer-centric, enabling banks to expose customer data, with customer consent, to third party providers via APIs

Okta and Cloudentity: The solution to simplify and accelerate adoption of PSD2 and Open Banking principles

With Okta and Cloudentity's integrated solution, financial institutions can quickly and safely comply with relevant regulations and position themselves to provide improved, secure, and seamless experiences for their customers. Here's how the leading identity management and dynamic authorization solutions work together seamlessly to help financial institutions adopt the Open Banking philosophy and deliver zero trust security, regulatory compliance, and customer innovation.

What Does This Mean In Practice?

Okta and Cloudentity work together to help businesses comply with the specific regulations of PSD2 and Open Banking standards.

Strong Customer Authentication

The PSD2 includes specific rules meant to define and strengthen multifactor authentication. All payments initiated by customers and exceeding €30, as one example, 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)

One feature of Strong Customer Authentication is dynamic linking. For payment transactions, the Okta + Cloudentity solution offers Strong Customer Authentication that links your transaction to a OTP code, to create a derived confirmation code linked to your transaction data—a truly unique code that can only be used to sign a specific transaction.

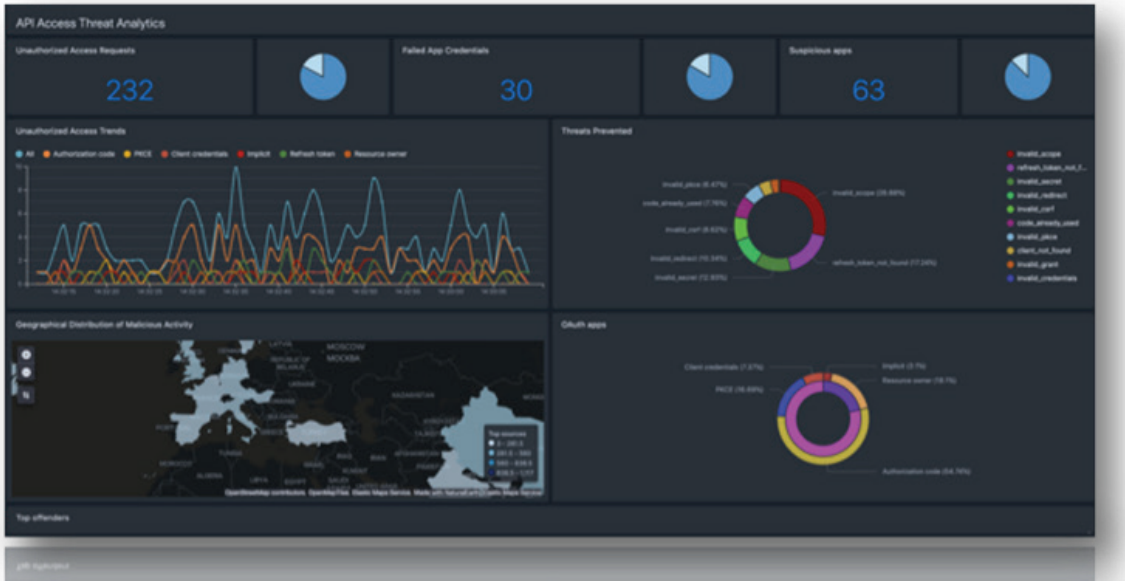
Solution:
Multiple Factors and Customer-Based Factor Control

The Okta + Cloudentity joint solution provides a range of factors for multi-factor authentication, including passwords, security questions, SMS, Voice, Email, Okta Verify, Google Authenticator, Yubikey, U2F, and biometrics. Organizations can choose the factors most appropriate to their needs and risk profile, and end-users, armed with self-service options to enroll and reset factors, can securely manage their experience without incurring additional support costs. Products like Okta Verify Mobile offer independent, out-of-band authentication methods to help prevent fraud, and admin dashboards let security operations teams centrally control and adjust policy without extensive developer cycles.

Transactional Risk Analysis

Because financial institutions and payment initiation service providers (PISP) will also be held responsible for monitoring and detecting unauthorized or fraudulent payments, integration with existing fraud engines and risk-based, transactional authentication and authorization solutions will become mission-critical. With pre-integrated patterns and advanced ML dashboards, banks can visualize real-time threats and changes in usage patterns. Paired with adaptive authentication, financial institutions can mitigate risk by understanding who—and, more importantly, what—is able to interact with APIs, workloads and data. This means assigning an identity to everyone and everything (no general service accounts) and understanding what those people, services and things are allowed to access with clear authorization and governance policies.

For transactions below €30 (our example), adaptive multi-factor authentication offers a non-disruptive method to reduce the risk of fraud. Leveraging a range of additional context such as user's device, device location, and IP, organizations can evaluate risk before accepting, and take automated remediative action like forcing step-up authentication or blocking the transaction.


API Access Threat Analytics
Unauthorized Access Requests
232
Failed App Credentials
30
Suspicious apps
63
Unauthorized Access Trends
Threats Prevented
Geographical Distribution of Malicious Activity
OAuth apps
Top offenders

Secure API Management

The Okta + Cloudentity joint solution provides AI-driven Dynamic Authorization and identity governance to help customers deliver secure Open Banking services. Automated governance and machine learning technology, powered by Dynamic Authorization and combined with a world-class Consumer Identity and Access Management (CIAM) platform, automates the onboarding of APIs and cloud services into Okta's ecosystem. These APIs and services are protected with dynamic access control policies pre-configured to meet the needs of specific industries like finance. The joint solution's API Access Management integrates with popular API gateways, including Apigee, Mulesoft, Amazon API GW, Azure API GW, SoftwareAg, Kong, and Tyk, allowing flexibility and supporting existing tech stack infrastructure.

Fine-Grained Consent Management

PSD2 & Open Banking requires user consent to authorize financial service providers to share information with 3rd party providers. This consent must be fine-grained and easily granted or revoked by users in a seamless experience, and any user changes to consent preferences must be reflected not only within the banking platform, but in all downstream 3rd-party providers as well. Our joint solution provides customer authentication products and directory solutions so you can store user records securely and manage a single source of truth for any and all consent changes.

The Okta + Cloudentity joint solution helps you meet PSD2 and Open Banking compliance. But it will also help you innovate the customer experience in a number of ways:

- Expand offerings, by opening APIs that connect your customers to other service providers
- Integrate services platforms such as mortgage brokers, pension plans, travel insurance, and wealth management services
- Create alliance partnerships and provide customers with a convenient aggregated view of their accounts thru partnering banks
- Receive and analyze customer behavior across solutions, developing profiles so you can provide more personalized and relevant services
- Digitize banking services while keeping your customers' PII and transactions secure

Go Beyond Compliance and Safely Build Better Customer Experiences

By utilizing Okta and Cloudentity's end-to-end solution, financial institutions can put themselves in a position to immediately tackle real world use cases below.

PSD2 and Open Banking will likely continue to evolve, with new requirements and concepts each bank will need to consider. But compliance is only part of the challenge. Whether they partner with FinTechs or invest in building out the infrastructure themselves, financial institutions need to seize this opportunity to reinvent the financial services marketplace. By leveraging partnerships like Okta and Cloudentity to safely create new products and services that delight and empower their consumers, banks can stay ahead of the competition, build customer trust, and assert themselves as a critical component of the new, consumer-centric future.

Secure Mobile & Online Banking Access

Unify customer identities by integrating your banking apps effortlessly. And ensure secure customer access to your online and mobile banking apps with frictionless strong customer authentication.

Remote Account Opening

Verify customer identities with identity proofing and strong customer authentication.

Call Center Verification

Use a wide range of authentication factors to smooth customer experiences while reducing fraud.

Payment Verifications

Stop fraud in its tracks and verify payment transactions with out of band authentication such as mobile push.

360 View of the Customer

Overcome organizational silos created by channel, product, geography, or business unit. Increase customer lifetime value by deepening your understanding of their interests and preferences.

Customer Privacy and Consent

Give customers full, centralized, fine-grained control over consent preferences at the data object level.

Open Banking/Third-Party API Management

Create new business models for your customers by allow securely exchanging data within the organization and across your ecosystem.

Secure Centralized Access to Partner Portals

Optimize end-user experience by centralizing their appropriate resource access in one secure personal portal.

Secure, Seamless Access for your Employees

Centralize identity management and establish a frictionless Zero Trust security posture.

okta | CLOUDENTITY

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 7,400 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, go to **www.okta.com**.

About Cloudentity

Cloudentity is a privacy-first Customer Identity and Access Management (CIAM) platform focused on providing the right people the right data at the right time and place. This is done through powerful, cloud-native identity and access control microservices that integrate quickly, seamlessly, and efficiently into an organization's existing hybrid, or cloud architecture. Cloudentity's API MicoPerimeter™ provides in-depth visibility, protection, and policy enforcement at the API level, securing web applications from malicious attacks. For more information, go to **cloudentity.com.**