PaymentsEd FORUM

Your source for payments education

Open Banking

PSD2, GDPR and the American Merchant

Scott Adams
Evolutioneer
FraudPVP

Rene Pelegero
President & Managing Director
Retail Payments Global Consulting Group

Agenda

Payment Services Directive 2 (PSD2) and Open Banking

- Key pillars
- PSD2 challenges & status
- Open banking globally
- Open banking in the USA

General Data Protection Requirements (GDPR)

- What is it? And why is it important?
- What's in scope
- What needs to be reviewed
- How it interacts with PSD2 & Open Banking principles

Effect on US Merchants

- The commercial benefits
- The operational practices needed to take advantage of those benefits
- The technical considerations to implement the operational practices

Key Pillar 1

Access to the Account

XS2A

Applies to all payment accounts issued to EU account holders which have digital access (e.g. web or mobile interfaces)

- Services to be provided:
  - Confirmation of account status and funds
  - Payment Initiation
  - Account Information

Account issuers (called Account Servicing Payment Service Provider or ASPSP) must provide secure communication channels to transmit data and initiate payments.

The default technology being adopted to provide access is the API.

PaymentsEd FORUM

Key Pillar 2

A new language:

CA = Competent Authority (Regulator)

ASPSP = Issuer of the account (Bank or Wallet)

PSU = Payment Service User or the owner of the account (Consumer / Business)

- XS2A:
  - PISP = Payment Initiation Service Provider
  - AISP = Account Information Service Provider
  - TPP = Third Party Processor

A company can perform one, two or all of the three roles, depending on it's product and appetite for regulation.

Key Pillar 3

Competent Authority

CA

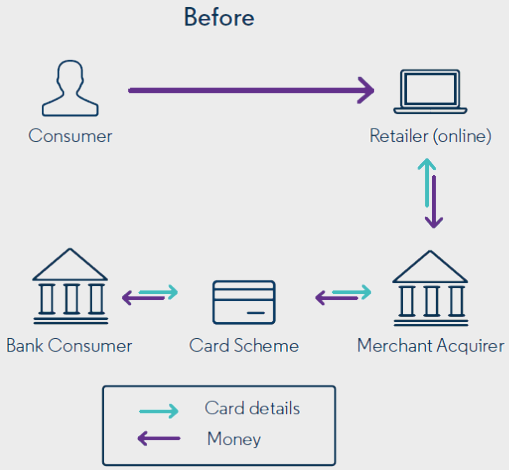
CA's are domestic regulators delegated the responsibility for overseeing the operation of PSD2. The FCA in the UK, for example.

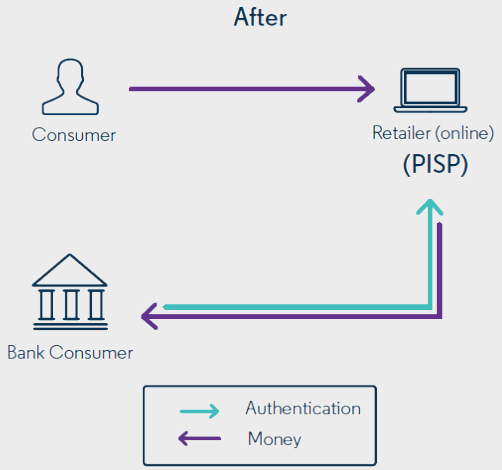
- Key Roles:
  - Ensuring ASPSP's (mainly Banks) comply
  - Certifying companies who want to use XS2A
  - Operating the Trust Centre infrastructure
  - Granting and managing exceptions

PSD2 clarifies the role and enhances the regulatory authority of CA's. Within this framework, the EBA will be charged with ensuring interoperability and consistency across the EU.

PSD2 Direct Access To Funds

- Direct access to bank accounts without intermediaries (XS2A)
  - Merchants become Payment Initiation Service Providers (PISPs)
  - Banks become Account Servicing Payment Service Provider (ASPSP)
- ASPSPs to develop and expose Application Programmatic Interfaces (APIs)
  - APIs defined by the European Banking Authority (EBA)
  - No sharing of bank login credentials to AISP





PSD2 Challenges

Timing

- Concerns around security, dispute management, the lack of standards and potential for negative consumer reaction suggest watch and wait.
- Against this, competitors may create a first mover advantage

EU / Global Adoption

- PSD2 is new to the EU and still rolling out, not widely implemented yet.
- Will it succeed?
- Will it spread around the globe?

Practical Questions

- Where to get the right advice?
- How to develop expertise?
- Who to partner with, in-house, Fintechs, Banks?
- Impact on existing Bank relationships?

Payment Services Directive 2 Status

Where are we now?

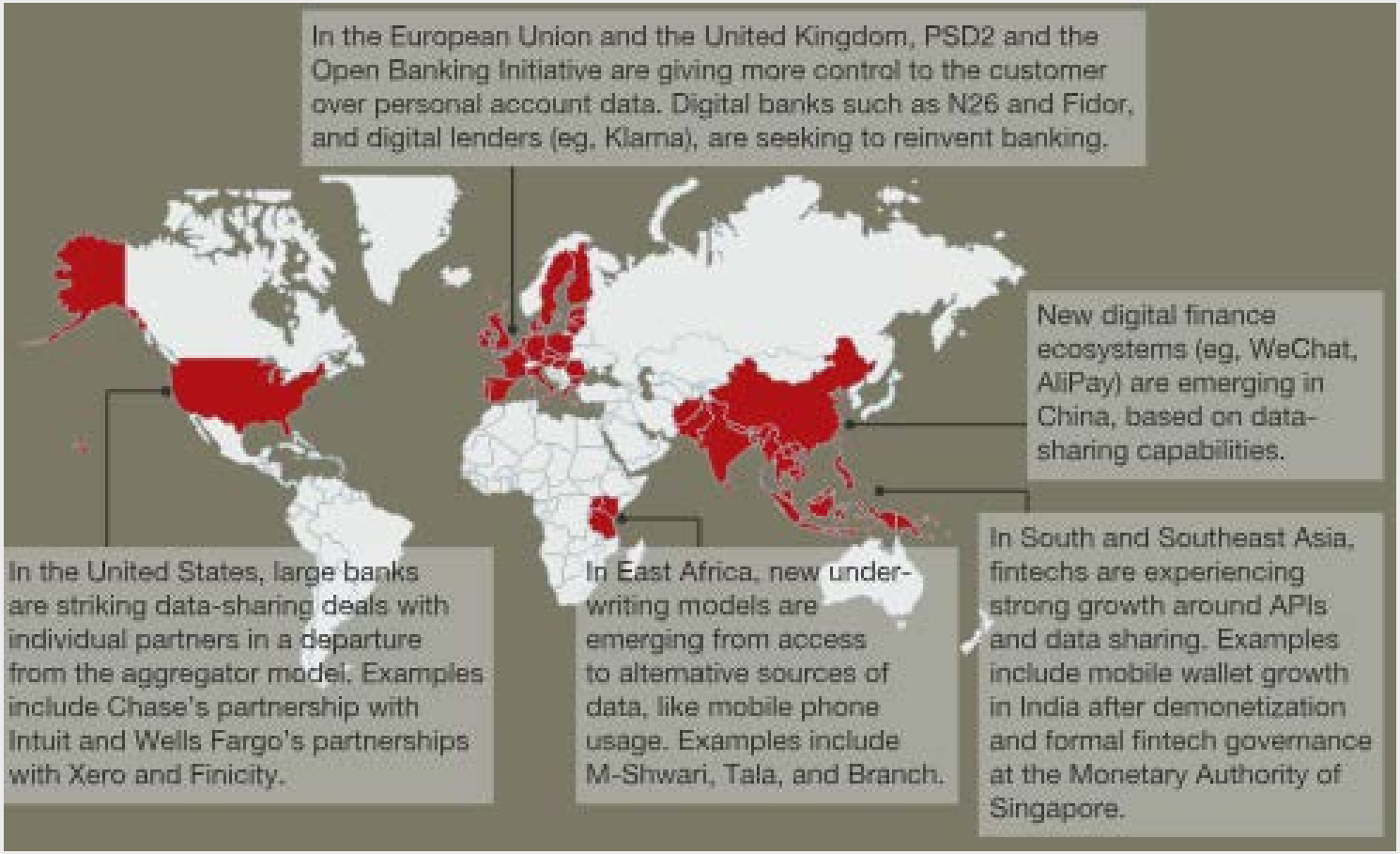
The big unknown:

Consumer acceptance and adoption

PSD2 is anticipated to be the first step on a journey towards wider Open Banking, with PSD3 likely to follow.

- Rolling implementation
  - Multiple countries missed the intended Jan 2018 deadline, including - NL / ES / PL / SE / AT
  - In the UK, only three big banks were ready on time, extensions were granted for others
- Standards
  - No pan-EU standards for interface design and performance
- Regulatory Technical Standard (RTS)
  - September 2019
  - Strong Customer Authentication (SCA)
  - User experience
- Exceptions
  - It is possible for a Competent Authority to grant exceptions to both account issuers and 3rd parties using Access to the Account

Open Banking Around the Globe



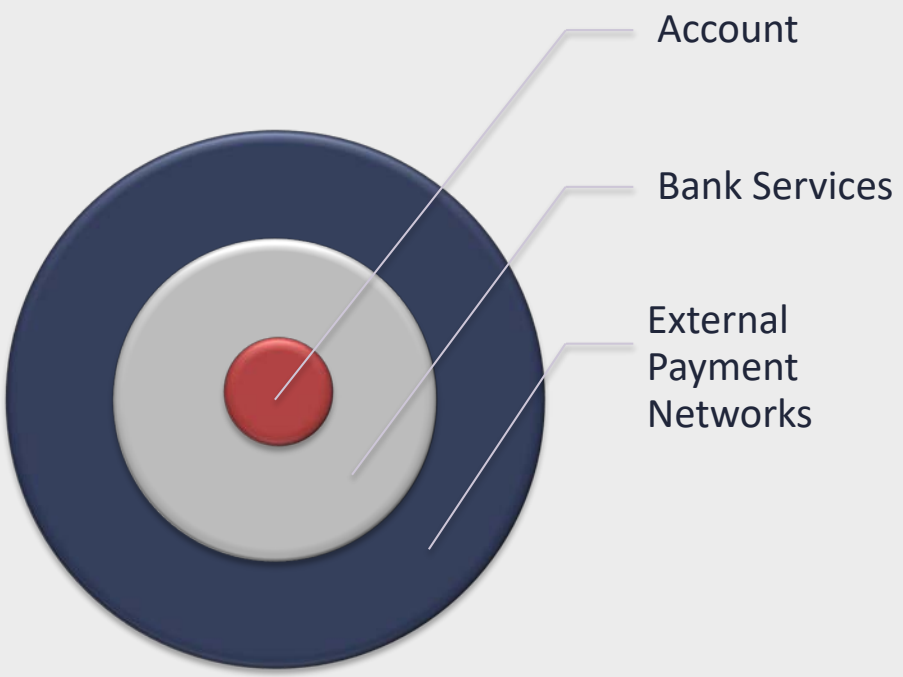
*** Source McKinsey Payments Practice**

Open Banking - general phrase used to describe banking assets and services which are exposed to 3rd parties and typically accessible via API.

PaymentsEd FORUM

Open Banking in the U.S.A.

- Access to bank accounts controlled by external payment networks
- Little motivation for introduction of innovative services



U.S. Open Banking Status

Adoption

- Majority of US Banks (53%) seem to consider Open Banking as critical to their digital transformation
- One-off deals
  - Wells Fargo & Xero
  - Chase & Intuit
  - Capital One
  - Bank of America
  - Screen scraping (e.g. Mint, Personal Capital, Yodlee, PaywithMyBank)

Challenges

- Lack of demand, standards, business case and urgency
- Concerns about security
- Conflicting requirements
- No appetite for top-down regulatory approach
- Effort cannot be ad-hoc or a non-scalable patchwork of one-off agreements

Way Forward

- CFPB data sharing guidance
- Conversation shifting from "who owns the financial data" to "how to enable" secure financial data sharing with third parties
- Standards are being set worldwide
  - PSD2
  - India
  - Australia

General Data Protection Requirements (GDPR)

General Data Protection Regulation

- New regulation changing the way data can be stored and used.
- Already in law
- Came into force May 2018

Impact

- Data belongs to subject
- Definition of personal data extended
- Applies to all EU citizens
- Trumps PSD2
- Consent to use data required
- New rights

Implications

- Opt-in will be default
- Strong consent procedures needed
- Non-resident companies with EU clients impacted
- Regulator has a big stick *(4% of global turnover or €20m)*

What is GDPR?

From the regulation:

The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business.

What are the key points?

- Covers all EU Citizen data
  - Applies to ALL companies inside and out of the EU
- Not Just PII per PCI
  - Hashing and encryption encouraged
  - Could include IP Address
  - Even online IDs
- Explicit Consent and Transparency in Data use

What are the key points?

- Rights of Data Subjects
  - Right to:
    - See Data
    - Correct Data
    - Restrict Portability
    - Completely Delete Data
  - Generally within 30 days
  - Right for Human Review of AI Decisions

What do we need to do?

- Review your data
  - Ask yourself
    - Do we need this? Default to no.
    - Can we hash it or encrypt it?
      - Hash if you never need the clear text value
  - Make sure to have View/Edit/Delete ability
  - Review Consent methods
  - Review T&C and Privacy Policies

What Does this all mean for U.S. Merchants?

Commercial Benefits

What are the commercial implications?

Are there obvious or potential benefits?

Operational Efficiency

Is there potential to create more centralized payment factory?

Will visibility of cash and cash flow improve?

Technical

- **What does a merchant need to do to realize the potential?**
- **Does this accelerate the shift towards IT driven payment operations?**

PaymentsEd FORUM

Commercial Implications

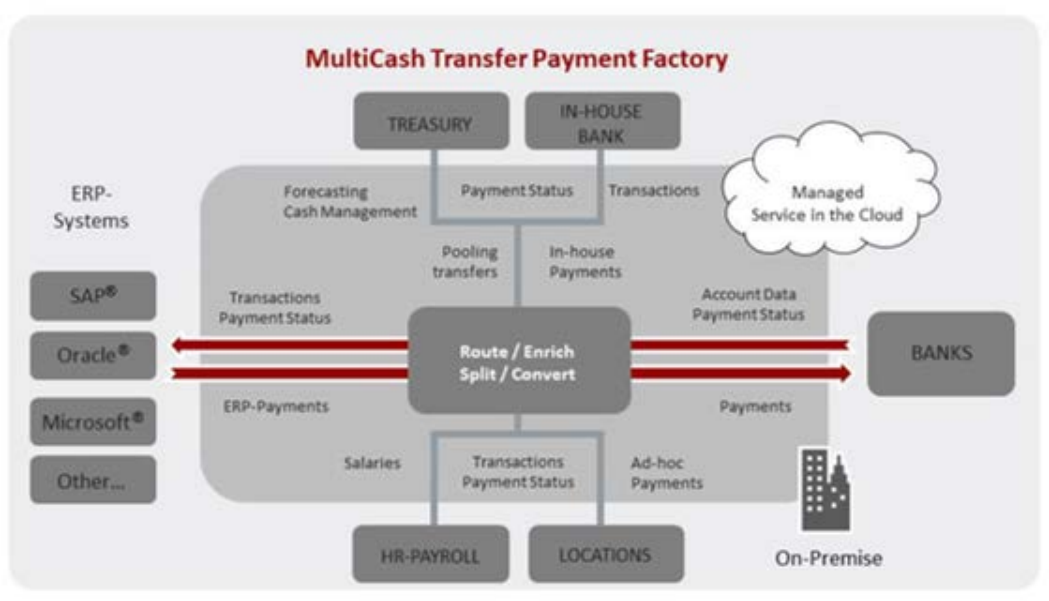
We Expect:

- Increased competition amongst PSP providers
- Changed relationships with consumers
- Changed relationships with Banks

Over time, payments and Banking services could become quite different as a result of PSD2.

- New consumer and corporate relationships
  - Account information access
  - Consumer buying pattern analysis
  - Better payment experience and loyalty schemes
- Merchants as Fintechs and other new payment entrants (TPPs)
  - Increases competition
  - Segmentation of specialized services
- Reduced dependence on payment gateways and SWIFT
- eCommerce for Merchants
  - New payment methods, gradually moving from dependence on card schemes to bank to bank
  - Lower acceptance fees for merchants

Operational Processes



*Source: Management Data Praha

- Enhanced multi-banking experience
  - Centralized payment factory concept
  - Dashboard
  - Real-time visibility
  - Removing the need for multiple Bank tokens
- Greater access to data and analytics
- Deeper integration can spill over to financial services and other product areas

Technical Considerations

- TMS & ERP
  - Merchants should be able to leverage existing systems and add middleware to connect directly to Banks
- Speed and responsiveness to the business
  - Should lead to faster implementation of new Banks and functionality
  - Quicker and more flexible access to new payment systems
  - More responsive to compliance and risk related issues

Summary & Key Takeaways

PSD2:
Pay attention and build a strategy

- Companies quick to adapt will realize greater operational efficiency and strong new data sources to better enable products
- Not widely implemented yet
- Concerns around security, dispute management, the lack of standards and potential for negative consumer reaction suggest watch and wait.

GDPR

- Explicit Consent
- Much stronger than PCI … could include IP and online IDs
- Must provide view/edit/delete
- Must be transparent
- Huge fines so be prepared

U.S. Merchants:
To Do List

- Socialize Payments as a Product or a revenue enabling function
- Implement tools that allow for Factory operations and quick bank integrations
- Implement strong data gathering and protection practices

Thank you

Don’t forget to submit your session evaluation!

Rene Pelegero
Retail Payments Global Consulting Group
President & Managing Director
renep@rpgc.com

Scott Adams
FraudPvP
Evolutioneer
scott@fraudpvp.com