Future of Banking: Digital and Regulatory
Link ‘n’ Learn
March 22, 2018
Welcome
Agenda & Deloitte presenters

Today’s agenda

1. Introduction & PSD2 regulatory context
2. PSD2 opportunities and impacts on Banking strategy decisions
3. Which technology to face those challenges
4. Conclusion
5. Q&A

Presenters

Xavier Turquin
Senior Manager
Moderator & speaker on Banking strategy
xturquin@deloitte.lu

Benoit Sauvage
Senior Manager
Speaker on PSD2 regulatory context
bsauvage@deloitte.lu

Andy Fossion
Consultant
Speaker on technology impacts
afossion@deloitte.lu
1. Introduction and PSD2 regulatory context
Our perspective on PSD2 requirements

Under PSD2, the regulated payment landscape is further expanded and new requirements come in place in terms of security, access to information and insurance.

**Terms & Conditions**

Terms and conditions (T&Cs) signed by the customer need to include more information on the PSP, the services provided, charges, communication and safeguards.

**Risk management**

Payment Service Providers need to have frameworks in place for managing risk, including mitigating actions and classification of incidents, which needs to be updated on a regular basis.

**Liabilities**

All parties need to ensure that payment transactions are appropriately executed, supporting payer or payee disputes. Liabilities are reduced from €70 to €50.

**IFR & Surcharging**

Surcharging is no longer permitted if the payment instrument already benefits from Interchange Fee Caps.

SHA becomes the default option for intra-EEA payments in EEA currencies.

---

**Strong customer authentication**

Significant implications for financial institutions and third party providers (TPPs) e.g. two-factor authentication.

Comprehensive annual reporting to the local competent authority.

**Access to accounts**

Banks must adopt EBA Regulatory Technical Standards (RTS) to open their platforms to TPPs for PISP and AISP services.

**PISP & AISPs**

Financial institutions will be required to support new Payment Initiation Service Providers (PISPs) initiating payments and provide transactional data to Account Information Service Providers (AISPs).

**One leg-out transactions**

PSD2 will apply to payment transactions where at least one of the Payment Service Providers (PSPs) is based in the EU, and EEA for specific clauses.

* PISPs and AISPs together are referred to Third Party Providers (TPPs)
Timeline for PSD2 implementation

PSD2 entered into force on January 13\textsuperscript{th} 2018 with an effective application date of the RTS on Strong Customer Authentication and Secure Communication for September 2019

The core of the Directive is to be transposed by the Member States by January 2018 and is immediately applicable to banks and payment institutions, including EBA secondary legislation (i.e. Guidelines on Management of operational and security Risks).

* RTS on Strong Customer Authentication & Secure Communication
Minimum actions to comply with January 2018 requirements
Short-term requirements & action plan

**Domain**

You are expected to...

- Be responsible for incorrectly processed payments, providing as well a complaint resolution procedure for the customer
- Put in place a comprehensive internal control framework and reporting to the competent authorities, including detection and classification of major operational and security incident
- Provide account information and customer protection information in a readily available, accessible and understandable format in the terms & conditions

- Ensure PSD2 compliance across any transaction that has at least one leg within the EU
- The obligation on transparency of conditions and information applies to transactions with one leg within the EEA as well

- Reduce consumer interchange fees to 0.3% and 0.2% for credit and debit cards respectively
- “Unblended” pricing, separating service charges from interchange and scheme fees
- Provide merchants for each type of payment the separation between merchant service charge, interchange fee and scheme fee

**…to this end you should**

- Review current risk frameworks and systems to include appropriate mitigation measures and control mechanisms in relation to payment processes risks
- Perform an annual risk assessment and provide an annual report to the authorities. In the case of a major incident, notify the competent authorities & relevant customer
- Set-up workflows to ensure reimbursement of payment amounts and related fees, charges or interests incurred by a consumer in an incorrect payment
- Select at least one Alternative Dispute Resolution procedure (ADR) entity and make the information available to the customer
- Respond to customer complaints within 15 working days

- Ensure all necessary information is provided at least in respect of their part of the transaction, regardless of the currency used
- Review corresponding bank strategies to ensure mutual compliance

- Implement the required caps
- Ensure that from a compliance and reporting side, relevant workflows are in place to ensure correct information to the relevant actors

**Expected impact**

<table>
<thead>
<tr>
<th>IT</th>
<th>Business</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Minimum actions to comply with Q2 2019 requirements
Mid-term requirements & actions

<table>
<thead>
<tr>
<th>Domain</th>
<th>You are expected to...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Set up a strong customer authentication system, through the use of minimum 2 features (knowledge, possession, inherence) to confirm customer’s identity and validate payments</td>
</tr>
<tr>
<td></td>
<td>• Ensure access to accounts in order for AISPs and PISPs to provide their services. As long as the bank only provides e-banking with consultation mode, the bank will have obligations towards AISPs only*.</td>
</tr>
</tbody>
</table>

* The Bank will have obligations toward PISPs only when providing online transaction services for its own customers.

<table>
<thead>
<tr>
<th>...to this end you should</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Review the current authentication procedures</td>
</tr>
<tr>
<td>• Amend the technical infrastructure and the operational workflows to adapt to strong customer authentication requirements</td>
</tr>
<tr>
<td>• Ensure the installation (and potentially the development) of suitable software modules (i.e. API exposed to PISPs and AISPs), with all related change management and process design aspects</td>
</tr>
</tbody>
</table>

Those requirements are described in the pending RTS on Strong Customer Authentication and Common and Secure Communication

<table>
<thead>
<tr>
<th>Pillar</th>
<th>Chapter</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enhanced security and authentication requirements</td>
<td>Strong Customer Authentication</td>
</tr>
<tr>
<td></td>
<td>Exemptions from SCA</td>
<td>How the authentication procedure should be designed, involving dynamic linking, requirements for SCA elements and reviews to ensure security</td>
</tr>
<tr>
<td></td>
<td>Protecting Personal Security Credentials</td>
<td>In what situation is access exempt from strong customer authentication</td>
</tr>
<tr>
<td></td>
<td>Common Secure Communication</td>
<td>How to ensure confidentiality and integrity of user’s personalized security credentials</td>
</tr>
</tbody>
</table>

Common and Secure Open Standards of Communication
Minimum levels of communication between TPPs and ASPSPs in terms of traceability, interface, session security and data exchange

| Expected impact |
|-----------------|---|---|
| IT | Business | Compliance |
| ✔ |  | ✔ |

© 2018 Deloitte
2. PSD2 opportunities and impacts on Banking strategy decisions
Disruption in traditional industries
Customers have quickly adopted new ways of consuming goods and services, completely disrupting whole industries

- Alibaba: The most valuable retailer in the world, has no inventory
- Airbnb: The world’s largest accommodation provider, owns no real estate
- Facebook: The world’s most popular media owner, creates no content
- Uber: The world’s largest taxi company, owns no vehicles

Coming soon?
The world’s largest financial services provider, holds no bank accounts

Financial Industry disruption has already begun
The directive has direct impacts in the banking industry, namely in the relationship between the banks and their clients.

**PSD2 – Key components**

- Higher variety of service providers
- Payment Initiation Service Provider role
- Account Information Service Provider
- Security requirements

**Market trends**

- Client expectations
- Monetization of data
- Third party ecosystem

The banking sector is forced to open their platforms through APIs, in order to provide access to information to TPPs, so far considered privileged.

**Open Banking** requires a rethink of the traditional banking business model, enabling banks to improve the customer experience. Banking actors that embrace this **new business model** will enjoy a significant advantage given their access to existing customers, strong brands and expertise.
The Directive accelerates the «Open Bank» movement and creates new market opportunities both for Banks, Fintechs and other non-financial players.
Risks for incumbent banks

Historical actors are pushed into changing their role in the financial services value chain while they struggle with the expected reduction in traditional revenue streams

### Changing the position in the value chain

<table>
<thead>
<tr>
<th>Before PSD2</th>
<th>After PSD2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Producers</td>
<td>E2E Player</td>
</tr>
</tbody>
</table>

### Reduction of the traditional revenue

1. **Transactions**
   - Decrease in transaction fees due to new regulation
   - Emergence of new players in the digital payments provision

2. **Cards**
   - Reduced card usage by pushing revenue associated with annuities and interchange
   - Preference for non-credit card payments

3. **Interests**
   - Preference for non-credit card payments

---

In case of absence of a response strategy, the **incumbent Banks tend to lose the distribution role** through their interfaces and to be forced into a position of solely producers of products and services

---

**Transparency of commissions in transactions**

- Comparison Tools
- Easiness in changing financial providers

© 2018 Deloitte
Strategic Decisions
The Bank’s way of acting in the open banking context will depend on its position on the value chain...

How do banks want to be positioned in the value chain?

Focus on the production

- Focus on the production of **financial products for third-party distribution**
- Create new revenue streams, by monetizing beyond-PSD2 APIs

Requirements

- Focus on efficiency, scale, risk assessment, product quality and pricing

End-to-end player

- Maintain the role of distributor and producer, leveraging their position though cooperation with other entities at all stages of the value chain

Requirements

- Focus on organizational structure, building internal capacity and cooperation with strategic partners

Focus on the distribution

- Focus on the relationship with the client, through the distribution of products and services of multiple providers

Requirements

- Continued investment in channels, counseling and service
Strategic Decisions
... and the scope of its offering

What products and services will the bank have?

<table>
<thead>
<tr>
<th>Traditional Financial offer</th>
<th>Global financial offer</th>
<th>Beyond-banking services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focus on traditional financial products</td>
<td>Focus on a global financial offer, leveraged by complementary services</td>
<td>Offer non-financial products and services, produced internally or by TPP</td>
</tr>
<tr>
<td>Make available only the mandatory APIs</td>
<td>Provide APIs beyond those requires by PSD2</td>
<td>Monetize supplementary APIs (i.e. monetization of aggregate customer data)</td>
</tr>
</tbody>
</table>

**Do Nothing**

**Beyond PSD2**

Traditional Private Bank moves to Open Banking and provides regulatory compliant financial services.

**Beyond Retail Banking**

Banking Assistant with Account and Card aggregation, and including “Max Services” like, train ticket, birthday gift, or administrative assistance.
Strategic Positioning

By combining different decision axes, it is possible to obtain alternative positioning scenarios.

- Define market patterns and make commitments to become a clear market leader.
- Actively participate in broader digital ecosystem.
- Actively create partnerships with FinTechs and other companies in order to add commercial value to the offer.
- Defend the relationship with the client.
- Implementation limited to the regulatory minimum.
3. Which technology to face those challenges?
Banking ecosystem evolution

The need for intelligent orchestration is not new, it appeared and increased with the evolution of the banking ecosystem.

- Life was easy
- More channels and customer systems
- Need for integration – an Enterprise Service Bus
- Need for intelligent orchestration

An Application Programming Interface (API) is a set of clearly defined methods of communication between various software components.”
An API-based architecture is characterized by several components such as:

1. A **Gateway** acting as the front-end, receiving and routing requests, dealing with security aspects, etc.
2. A **Portal** listing services available and allowing users to subscribe/access them.
3. An **API Management** component which is the core component interacting with features and backend systems.
4. Other **Common Features** shared among all other components. Those features are generally provided by an API Management solution selected to implement an API-based architecture.

**Sample of high-level API-based architecture for a bank**

<table>
<thead>
<tr>
<th>Merchants</th>
<th>Retailers</th>
<th>Partners</th>
<th>Customers</th>
<th>Credit card providers</th>
<th>Startups / FinTechs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>API Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quota management</td>
<td></td>
<td>Authorization / Authentication</td>
<td>Sandbox management</td>
<td>API reporting and Analytics</td>
<td>Core systems</td>
</tr>
<tr>
<td>Orchestration / routing</td>
<td></td>
<td>Service catalog management</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2018 Deloitte
Key benefits of API management

API Management provides key benefits both from an internal and external perspectives.

<table>
<thead>
<tr>
<th><strong>External Benefits</strong></th>
<th><strong>Internal Benefits</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Integration with 3rd Parities</strong></td>
<td><strong>Compliance</strong></td>
</tr>
<tr>
<td>APIs can act as critical components of 3rd party services, providing organizations with entirely new distribution channels and the potential to expand their reach beyond the immediate customer base.</td>
<td>Reusability and consistency are core characteristics of API design, and facilitate the ability to apply universal governance measures from a centralized platform to ensure compliance.</td>
</tr>
<tr>
<td><strong>External Collaboration</strong></td>
<td><strong>Innovation</strong></td>
</tr>
<tr>
<td>API standards are increasingly evolving towards a universal format that is vendor neutral, portable, and open. This “common tongue” provides access to an ever-expanding body of use cases, development materials, and talent.</td>
<td>Making digital services publically available opens a channel for third parties to experiment and develop innovative new products without requiring any financial investment or risk, effectively crowdsourcing innovation.</td>
</tr>
<tr>
<td><strong>Internal Collaboration</strong></td>
<td><strong>Internal Collaboration</strong></td>
</tr>
<tr>
<td>The “plug-and-play” nature of APIs fosters the ability of teams working on separate systems or projects to easily link or incorporate each others’ solutions.</td>
<td></td>
</tr>
</tbody>
</table>

© 2018 Deloitte
Main PSD2 standards
France, Germany and UK have started to build their own standards to support compliance with PSD2

STET (France) / The Berlin Group (Germany)
Both standards have been initially defined by consortiums of banks with the objective to align payments processing. They are now being extended to cover broader services, in particular related to PSD2, with the aim to target new businesses.

Open Banking UK
Created in 2010 with the CMA9 bank, this standard aims at covering a broader scope than PSD2 in particular regarding user experience.
Financial API world
FinTechs have already took the opportunities offered by APIs by using them to propose products and services

API connectivity

- Account aggregation / PFM
- Payments & Remittance
- Cash and Treasury management
- Identity & KYC
- E-invoicing
- Loans
- Robo-advisory / Investments

NON EXHAUSTIVE
4. Conclusion
Future of Banking
What are the questions to consider to live in the future open banking world

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Risk</th>
<th>Data and technology</th>
<th>Leadership and culture</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What are the risks that open banking could pose to your current business model?</td>
<td>• Do you understand the (additional) cyber and fraud risk associated with this opening up of customer data?</td>
<td>• Do you have the data capability to fully exploit the opportunities from the opening up of customer banking data?</td>
<td>• How can your leadership help facilitate an ‘agile’ and pro-innovation culture across the organisation from the top down?</td>
</tr>
<tr>
<td>• What is your bank’s API strategy?</td>
<td>• Do you understand the conduct risk associated with potential propositions?</td>
<td>• Are your back-end systems robust enough to enable winning open banking propositions?</td>
<td>• How can your organisational structure become more ‘agile’? How can you erode barriers between department and product ‘silos’?</td>
</tr>
<tr>
<td>• What are the opportunities to go beyond simply complying with open banking regulation?</td>
<td></td>
<td>• What role can RPA and cognitive tools, and distributed ledger technologies, play in helping you adapt to this future?</td>
<td>• Where are the opportunities to collaborate with FinTechs to drive efficiencies/improve propositions?</td>
</tr>
<tr>
<td>• In which products and in which segments of the value chain should you be focusing your open banking investment?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
“Banking is essential, banks are not.

Bill Gates, 1994
5. Q&A
Next Link’n’Learn

Date: Thursday 12\textsuperscript{th} April 2018

Topic: GDPR from different perspectives
Deloitte is a multidisciplinary service organization which is subject to certain regulatory and professional restrictions on the types of services we can provide to our clients, particularly where an audit relationship exists, as independence issues and other conflicts of interest may arise. Any services we commit to deliver to you will comply fully with applicable restrictions.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries bringing world-class capabilities, insights, and high-quality service to address clients’ most complex business challenges. To learn more about how Deloitte’s approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.