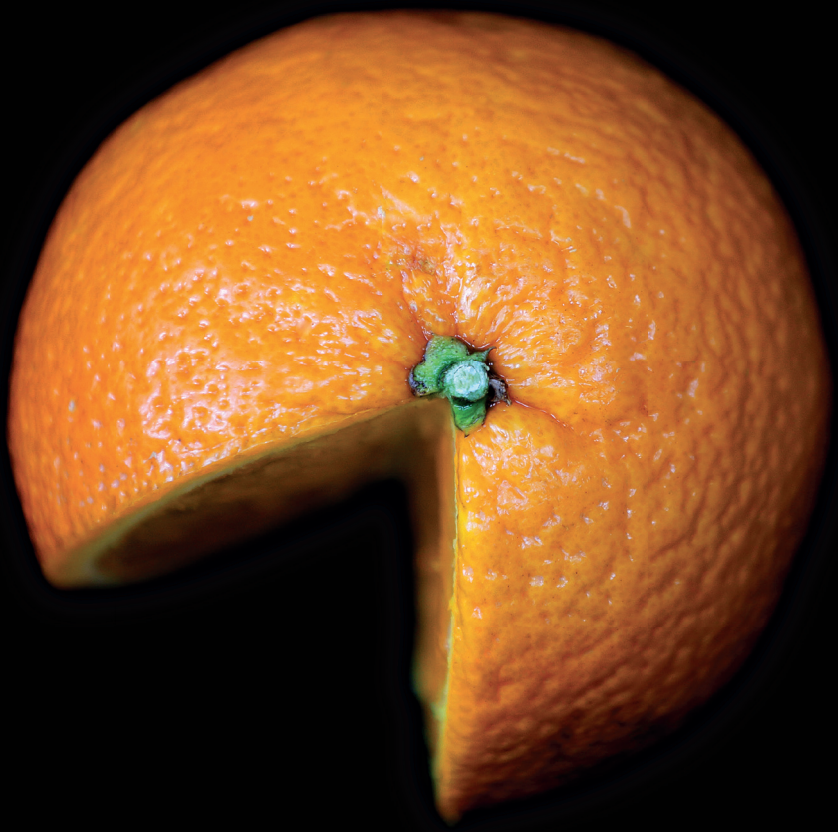
Deloitte.



European PSD2 Survey
Results highlights

October 2017

Overview

Overview

The survey

- Over August and September 2017, we conducted interviews with our clients' across Europe to gather their views on the revised Payment Services Directive (PSD2) and how they are responding, from both a strategic and compliance perspective.
- We surveyed 70 firms across 18 European countries.
- 89% of firms surveyed were banks, building societies or other credit institutions. Most were universal or predominantly retail focused, with a more limited number being focused on corporate and institutional banking.1
- Respondents were drawn from a wide variety of senior roles. Most common were 'heads of' business lines, but also PSD2 programme leads and Project Managers (PM).
- The survey was structured in five sections:
    1. General background
    2. Third Party Access to accounts
    3. Strong Customer Authentication
    4. Strategic response to PSD2
    5. Final thoughts
- As usual in all surveys, not all respondents provided responses to every question. To bring out the most useful insights, the summarised results represent the proportion of actual responses, and any "no response" is excluded from our analysis.

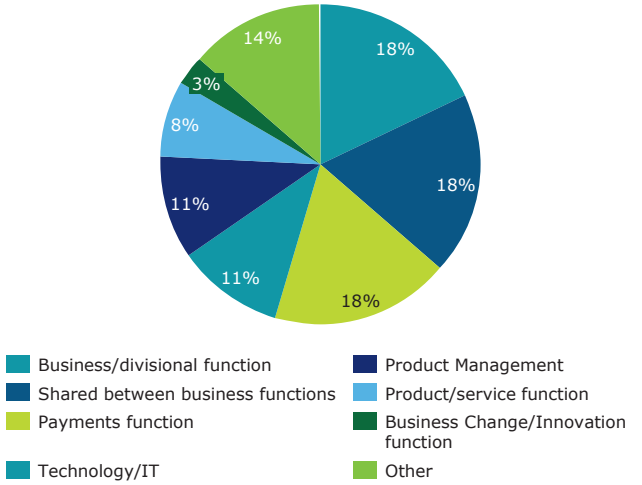
Results highlights

- Most firms are approaching PSD2 as on opportunity, although they remain very aware of the threats it poses to their business models.
- From a strategic perspective, whereas most respondents have performed some level of strategic assessment of the impacts of PSD2, the depth and extent of these assessments varies widely.
- This is reflected in the fact that only a quarter of firms feels ready and confident about their strategic plans, or have secured adequate budget and resources to develop them appropriately.
- Most resources, both human and monetary, have so far been devoted to responding to PSD2 from a compliance rather than a strategic perspective.
- Compliance wise, the majority of firms feels confident they will be ready when PSD2 goes "live" next January. However, a significant minority still has substantial work to do.
- Some of the key challenges, shared by most respondents, include:
    - The lack of a finalised Regulatory Technical Standard (RTS) on Strong Customer Authentication and Secure Communication
    - The lack of common Application Programming Interface (API) specifications
    - Liabilities under the Third Party Access model
    - Maintaining a positive user experience when applying Strong Customer Authentication (SCA)

General Background

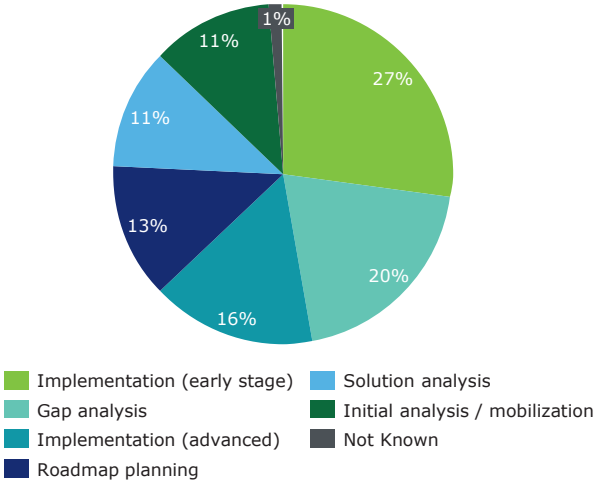
General background questions

Which organisational unit in your business is primarily responsible for addressing PSD2?



- PSD2 has broad organisational impacts, and this is reflected in multi-functional ownership approach.
- Responsibility for implementation is commonly shared between different functions, typically between payments and the business/divisional functions.
- Product Management and similar functions have a strong role in many respondents; their wide-ranging responsibilities organisational visibility make them well placed to understand wider impacts and implications.
- Legal, risk, compliance and regulatory change were significant ownership minorities, especially in larger banks.

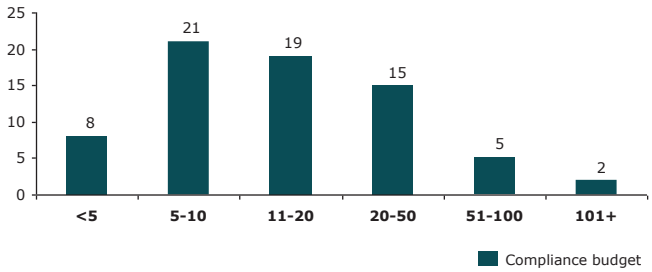
At what stage of progression is your organisation's PSD2 programme?



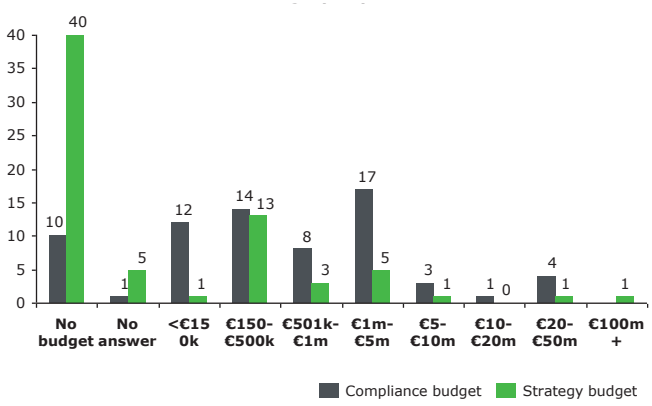
- As expected a large number of respondents were in the process of implementation; around 43% at time of interview, although this will have since increased.
- However, surprisingly the majority (57%) was still in pre-implementation stages, with the proportion of banks and non-banks roughly equal.
- This reflects a mixture of factors: some have struggled with the complexity of the analysis, others have fewer compliance requirements to fulfil.
- However, it suggests a busy end to the year for many organisations, and potentially a struggle to meet regulatory deadlines.

Resources and budgets

How many people are dedicated to supporting your psd2 implementation programme?



How many people are dedicated to supporting your psd2 implementation programme?



Resources

- The number of people supporting implementation programmes varied significantly depending on organisational size, and the size of the market.
- Most large and medium sized banks have between 11 and 50 people supporting their PSD2 programme

Compliance budgets

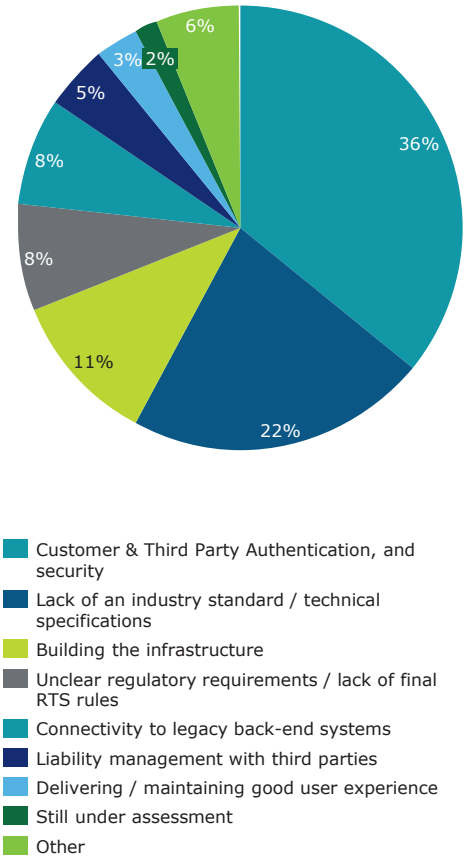
- 67% of respondents had a compliance budget of less than €1m.
- In Western Europe, ~40% of respondents had a budget of €1-10m, and ~13% a budget of €20-50m.
- Around one third of respondents, particularly within Central & Eastern Europe, had a budget of less than €500k.

Strategy budgets

- Interestingly, 57% of respondents had no budget currently assigned for responding to PSD2 from a strategic perspective.
- Whilst many have commenced strategic thinking, few organisations had committed and confirmed funding for a strategic response.
- Whilst there is significant industry discussion about the threats and opportunities presented by PSD2, few boards have committed funds yet.
- A number of respondents were in the process of preparing financial plans and would shortly be submitted to Boards, or executive committees, but the majority were not yet at this stage.

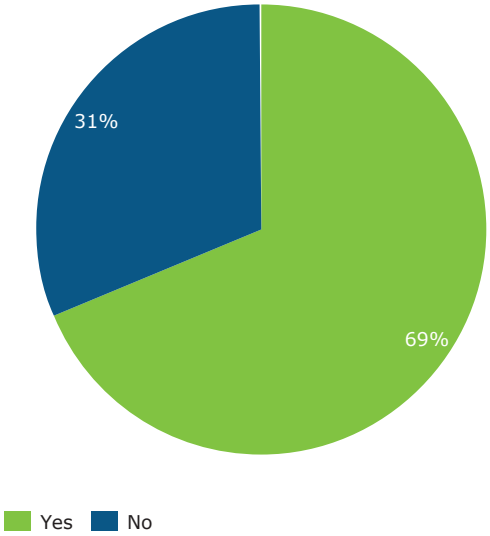
Third Party Access to Accounts

What do you consider to be the biggest challenge for developing a Third Party Access solution?



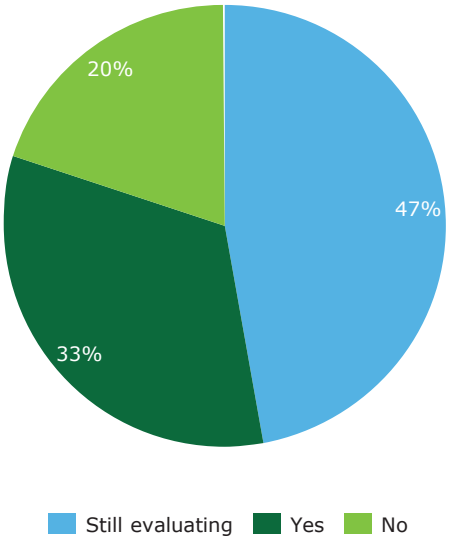
- A wide range of responses were provided, reflecting the fact that each organisation has unique challenges given their individual circumstances.
- **Top concerns** included:
  - Security and the authentication of customers and third parties.
  - The lack of clarity and definition within the RTS and/or API specifications.
  - Building and integrating the connectivity of the APIs into internal systems and infrastructure.
  - Liability versus third parties, as there is a significant market concern that the Account Servicing Payment Service Providers (ASPSPs) / Third Party Providers (TTPs) liability model is still unclear and untested.
- Around two thirds of respondents did not cite API connectivity to be a significant concern, thus debunking the idea that banks 'cannot do APIs'.
- Challenges are more specific security concerns reflecting the difficulty in appropriately applying API concepts and data access in a highly regulated environment dealing with highly sensitive data.
- **Other important challenges:**
  - How to appropriately design, implement and manage API and Open Banking governance processes for new strategic API platforms.
  - How best to design and maintain the user experience when implementing third party access.
  - Technical challenges around the lack of clarity on the European Banking Authority (EBA) register and certificate management for third party identity.
  - Unclear regulatory requirements especially, but not only, in the in the interim period (from January 2018 to when RTS on Strong Customer Authentication and Secure Communication takes effect).

Are you currently participating in any collaboration to define a collective approach to third party access standards?



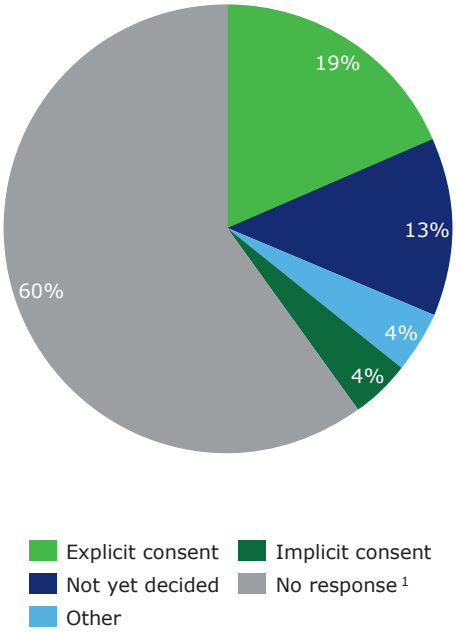
- **69% of respondents are currently participating in a collaboration** or standard setting body for third party access standards. These standard setting bodies included:
  - BIAN
  - Bundesverband deutscher Banken
  - CAPS
  - EBA Working Groups
  - ECB PIS Forum
  - PRETA
  - SETT
  - The Berlin Group
  - UK Open Banking Group
- Country (or regional) level initiatives operated by banks or financial sector organisations are in place in the following countries: Belgium, Croatia, Czech Republic, Germany, Hungary, Latvia, Poland, Romania, and Slovakia.
- Of the 31% of respondents not currently participating in a collaboration body, the majority were not aware of a local initiative in their local market. Roughly equal proportions were still evaluating or had decided not to participate.
- This suggests a **very strong industry demand for common standards and collaboration**, motivated by several factors, including:
  - The desire to reduce the individual burden to understand, develop and implement standards.
  - A recognition that common standards will facilitate overall adoption and increase the success of industry open banking initiatives.
- Market actors in several countries are beginning to explore the potential for **private sector 'central infrastructure' style hubs** to allow interconnectivity between market participants, and reduce development costs.

Do you intend to take a different approach to providing Third Party Access services for different market segments?



- Almost 50% of respondents are still evaluating whether to differentiate their services to different customer segments.
- There may be an opportunity for organisations to develop compelling targeted solutions and gain market share in certain market segments.
- Many respondents plan to begin with a basic, undifferentiated, approach and potentially then develop once the compliance requirements have been met, and market responses and demand is clearer.
- A significant proportion of respondents intend to build a flexible API platform architecture to support this, i.e. building platform foundations in a way that allows scalability and further development.
- Of those who intend to differentiate, the following plans were cited:
  - Differentiation particularly between Retail and Corporate/Business customer offerings, reflecting the different needs of these markets, and the potential use cases.
  - Offering 'premium' API services on top of basic compliance requirements to try to monetise access, or offer better and more compelling customer propositions.
  - Looking to partner with third parties or other organisations to build premium services.

How do you plan to deal with requirements around customer consent under the Third Party Access to Accounts model? How do you see the interactions between PSD2 and GDPR in this area?

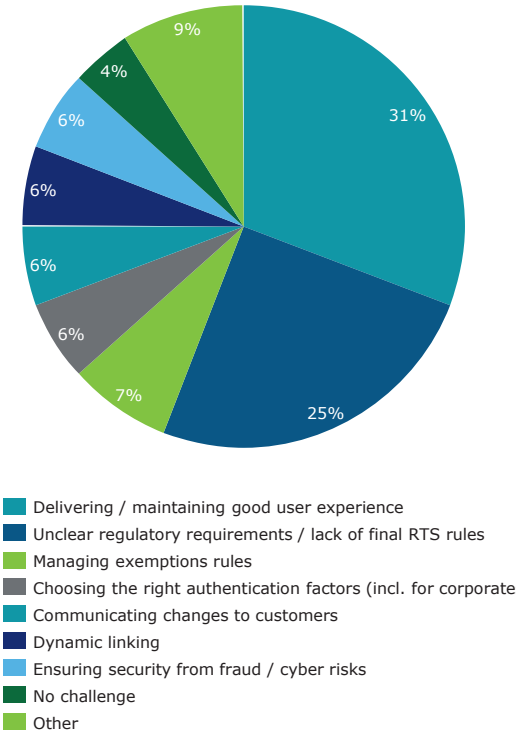


- There was no single clear majority view, reflecting the ambiguity in the requirements around consent.
- There is significant industry debate over which of the following consent models is required under PSD2:
  - '**Implicit consent**': where explicit consent is to be provided only to/ through the TPP and the ASPSP relies on and trusts this without obtaining direct consent from the customer.
  - '**Explicit consent**'; where the APSPS can/or should gain direct consent from the customer in addition to, or as a pre-condition, to the implicit consent provided by the TPP.
- Many banks intend to opt for the explicit consent model as this provides them with the most protection.
- Many intending to create a 'consent management' utility to allowing customers to turn on/off TPP access, view and manage consents granted.
- Several respondents highlighted the interaction, and some the potential tensions, between PSD2 and GDPR. There remains significant debate around the interactions between PSD2 and GDPR, with many seeing no conflict or believing PSD2 'trumps' GDPR.

1 This is the only survey question for which "no response" are included in our analysis, as the represent a significant proportion of the results. We believe it is likely the low response rates can be attributed to the current lack of clear views on this issue and/or of a finalised approach.

Strong Customer Authentication

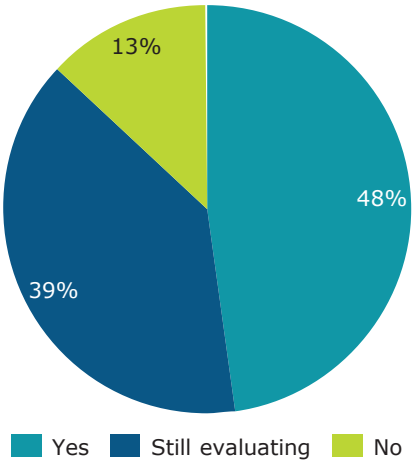
What do you see as the biggest challenge for implementing the Strong Customer Authentication (SCA) requirements?



- Respondents seem relatively less concerned over the implementation of the SCA requirements than Third Party Access.
- This is partly because many respondents already implemented security improvements to respond to the EBA's 2015 'Guidelines for the Security of Internet Payments'.
- However, as with Third Party Access, there were a range of different responses, reflecting each organisation's unique challenges and individual circumstances. The top two concerns, expressed by 56% of respondents, were included:
  1. How to maintain a **positive user experience** when applying SCA, particularly in conjunction with the exemption rules.
  2. The **difficulty of interpreting regulatory requirements and the lack of a finalised technical standard**. Many believe the principle-based approach creates ambiguity and uncertainty in implementation.
- Maintaining an understandable **customer journey and experience will be very important.** In particular helping clients understand why they are being asked for SCA in some cases and not in others will be essential.
- Several respondents noted that an element of **positive friction** in the experience could encourage customer trust and adoption, as it demonstrates controls are in place to safeguard customers against fraud and cyber crime.
- The **complexity of the exemption rules** was another commonly cited concern, partly due to the elaborate logic required, as well as ambiguities in the standards.

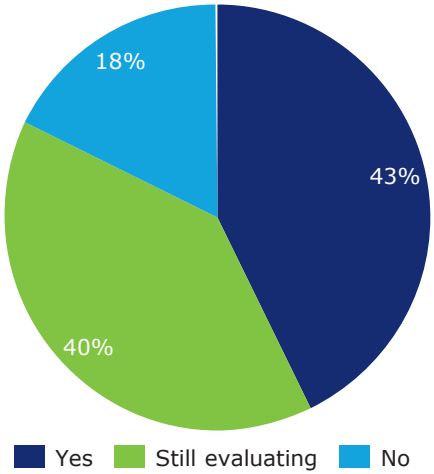
Strong Customer Authentication

Do you plan to utilise the exemptions from Strong Customer Authentication, particularly around Transaction Risk Analysis?



- Around **40% of respondents are still evaluating** whether to utilise the Transaction Risk Analysis (TRA) exemptions.
- 79% of those who already decided intend to utilise the exemptions, with only around 21% planning not to.
- However, many of those who plan to utilise the exemptions intend to take a **cautious approach to implementation, running pilots** before rolling out in full and to high value payments.
- Ongoing evaluation measures will focus on both customer experiences and fraud issues.
- Respondents noted that TRA implementation can be complex and challenging, although much depends on the sophistication of existing fraud screening capabilities.

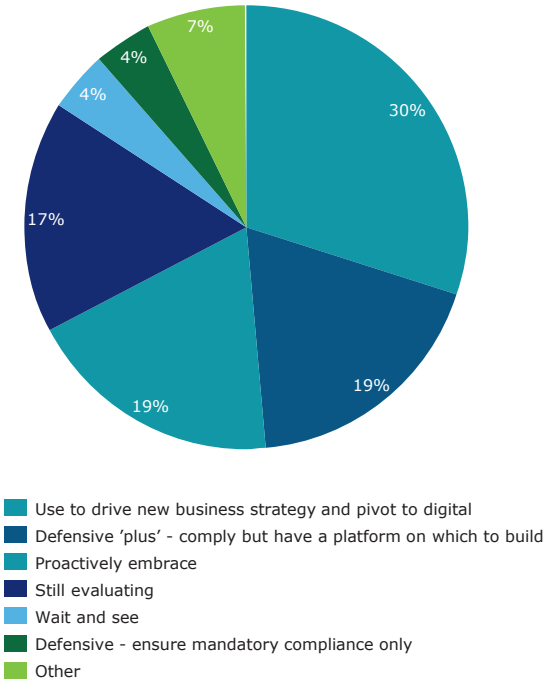
Do you intend to make any changes to your existing authentication techniques to respond to PSD2?



- 43% of respondents intend to make changes to authentication techniques, with 40% still evaluating. Only 18% currently intend to maintain their current processes.
- The main trend appears to be to **towards software/app based approaches and away from existing hardware-based solutions,** which are perceived as less user friendly.
- Most respondents appear to be opting for **'possession' as the second factor** over 'inherence' at this stage.
- Those intending to use biometrics mostly intend to use relatively mainstream methods such as fingerprints.
- 'Device as a factor' biometrics are starting to gain interest: allowing identification of users through the information gathered by mobile device sensors.

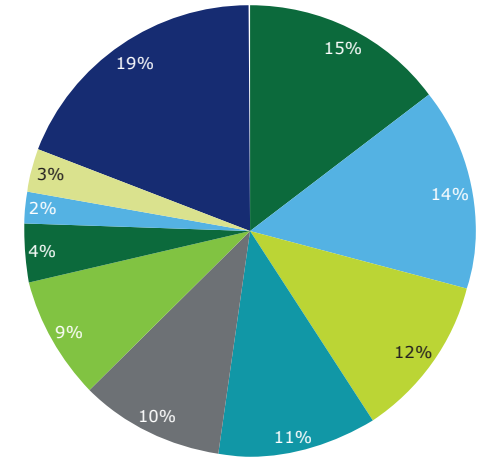
Strategic Response to PSD2

If you organisation has undertaken a strategic assessment of the impacts of PSD2, how would you characterise your response?



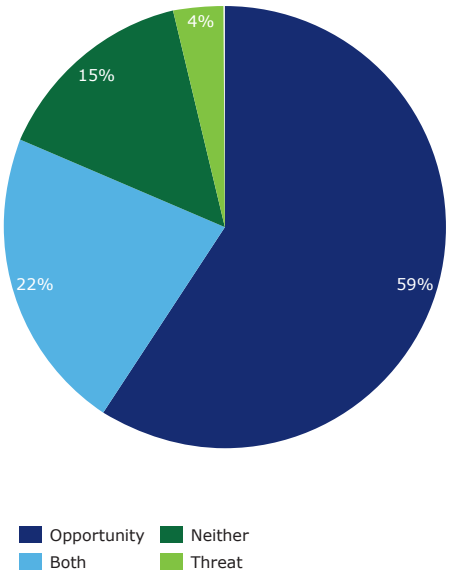
- Most respondents have performed some level of strategic assessment of the impacts of PSD2, and are aware of the threats and opportunities arising from PSD2.
- Many have identified some form of high level positioning they would like to pursue, however the **depth and extent of these assessments varies widely.**
- Around half of respondents characterised their response as **'Proactively embrace'** or **'Use to drive new business strategy and pivot to digital',** suggesting a significant proportion of organisations intend to pursue some form of **positive strategic response.**
- However, relatively **few respondents have performed a detailed assessment** of what they want to do, how they will do it, or have senior management buy-in and support for their strategy.
- Around 19% wish to pursue a defensive 'plus' strategy, i.e. to comply but have a platform on which to build, reflecting the fact that many are currently focused on mandatory compliance but want to keep their options open for the future.
- This confirms the view that **many see PSD2 as a long-term** trend that needs to be responded to, but that they do not necessarily wish be early movers or adopters.
- A significant proportion want to be able to 'react quickly' should a market opportunity arise, reflecting organisational needs to try and re-coup some of the significant investment made in API architecture.
- Around 19% of respondents characterised their response as 'Wait and see' or 'still evaluating'.

Do you plan to go beyond minimum compliance with Third Party Access requirements to take a more strategic response?



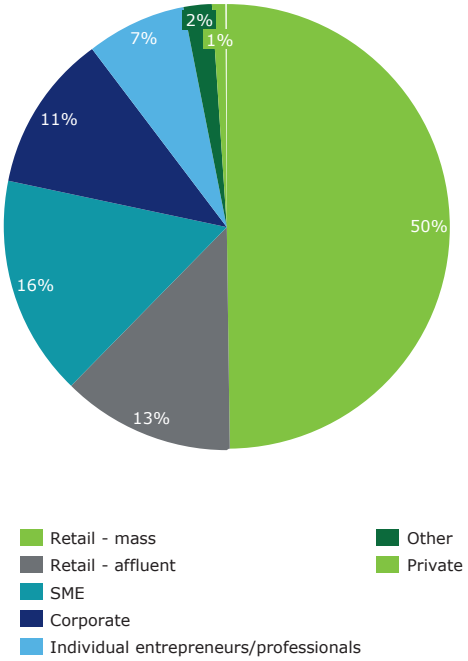
- Overall there is a **clear desire to go beyond the minimum compliance approach,** with 95% developing a strategic response.
- However, this does not correlate with other questions regarding strategy setting and investment, suggesting that currently **many plans are aspirational rather than concrete.**
- Common interests and desires included:
- Becoming a Payment Initiation Service Provider (PISP) or an Account Information Service Provider (AISP) amongst 19% of respondents suggesting such offerings could be widespread.
- Offering 'premium' APIs by 15% of respondents, a further 14% intending to launch new products and services, and 10% to offer additional non-payment services through APIs.
- Interest in partnering with FinTech's or other organisations amongst 35% of respondents. This may represent a significant opportunity for non-bank providers to work with the banks to introduce these services.
- Several respondents are talking to other product lines owners (such as lending, savings etc.) to determine what value API access and data services could bring to non-payment offerings.
- The partnering trend correlates with recent trends amongst **FinTechs to pivot towards more B2B business models**, partnering with the banks to access their customer pools due to the difficulty in trying to commercialise and build scale on their own.

On balance do you perceive PSD2 to be a strategic threat or opportunity for your organisation, and why?



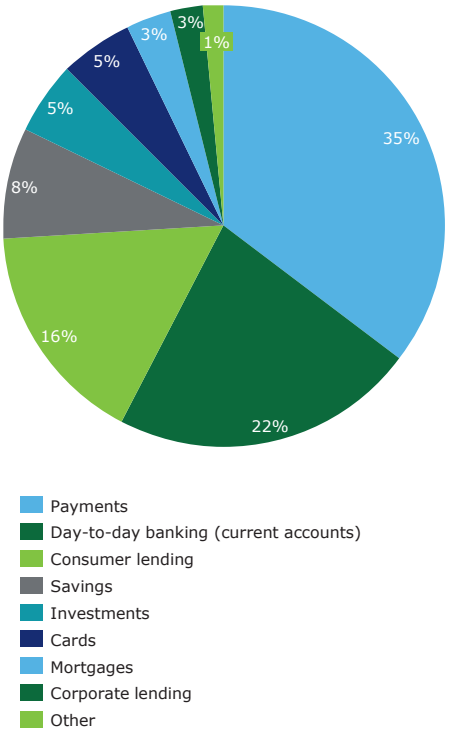
- On balance, a clear majority (59%) see PSD2 as an opportunity, but there is widespread acknowledgement that PSD2 is also a potential threat, and that in order to be an fulfil the opportunity organisations must prepare and react appropriately.
- This underlines the importance of a clear strategy.
- For those that see PSD2 as an **opportunity**, the top reasons were :
  - Banks will potentially have access to more customer data points, allowing better understanding of their clients, the ability to create more targeted offerings, and improve products.
  - It offers an opportunity to grow market share, or to grow share of wallet for existing customers.
  - PSD2 can be used as an internal catalyst to deliver infrastructure changes, which have been long desired but not had sufficient backing.
  - Non-bank providers typically see themselves as less of a target themselves for third party services, providing upside potential to move into the market to target others.
- For those that saw PSD2 as a **threat**, the top reasons were:
  - Many believe PSD2 is more of a threat for smaller organisations as they do not have the scale, strength of brand or financial resources to capitalise and respond in the same way as larger organisations.
  - Cards businesses are obviously concerned over revenues, particularly the potential for PISP services to substitute for Card transactions.
- Smaller and medium sized organisations recognise that PSD2 is a mixture of opportunities and threats. Given their relative size, scale, and limited financial resources, they need to take a clear view on areas in which they can realistically win and those in which they will need to partner.

In which customer or market segments do you think PSD2 will create the greatest threat or opportunity, and why?



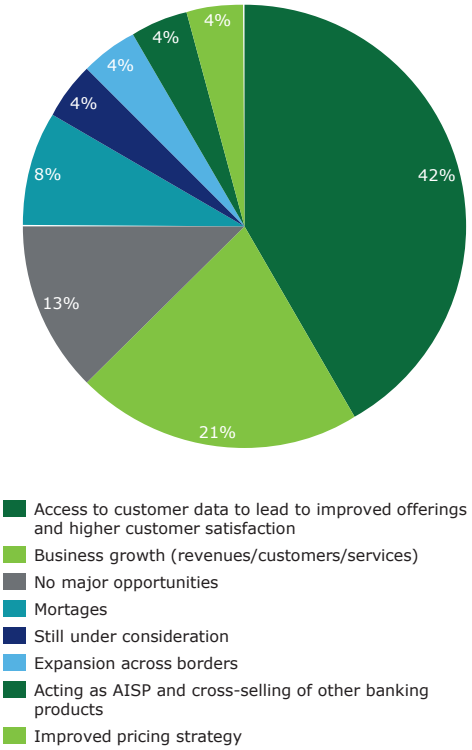
- **Retail banking emerged as the clear winner** for where greatest opportunity lies, with 63% of respondents identifying this sector.
- Several respondents commented on the potential to open up 'private banking' style services to mass retail and affluent consumers.
- Small and Medium Enterprise (SME) and Business Banking markets are also seen as an opportunity by around 27% of respondents.
- Many commented that PSD2 offers the **potential to offer services to SMEs** that would typically be reserved for larger corporates.
- There is a feeling that **PSD2 could 'democratise' access to services** that were typically reserved for the very wealthy (through Private Banking) or for large corporates, in the same was as 'robo-advice' has provided broader access to the investment management market.
- Corporate banking is generally seen as much less of an opportunity, primarily because PISP and AISP services are similar to services that large corporates can access today, and due to the perceived lower likelihood of Corporates to use third party services.
- Wealth Management and Private Banking services are also not perceived to be significantly threatened, for the same reason, as well as that the generally smaller size of the customer book will not be as attractive for third parties to target given build and pursuit costs.

In which product or offerings areas (existing or new) do you think PSD2 will create the greatest threat or opportunity, and why?



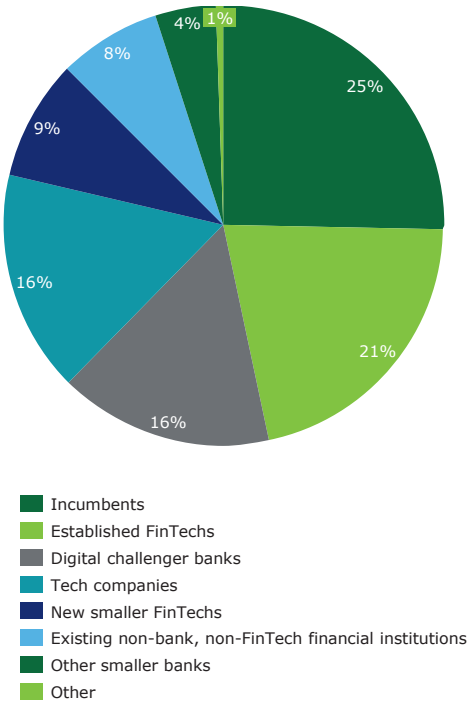
- **Payments** is the clear front-runner along with **day-to-day banking services.** This is in line with expectations, given the scope of PSD2 and the likely targets for AISP and PISP services.
- **Consumer lending was identified as an opportunity** by a significant proportion of respondents. The use of AISP services and data analytics to enhance decision making around lending risk is a potential benefit.
- Having a greater level of understanding of customers and the ability to more accurately analyse their true financial position using real-life data may allow **better calculation of credit risks.**
- In addition to making better decisions, it may allow credit to be offered to groups and segments that would traditionally have struggled to access it (e.g. the self-employed, new businesses, small businesses etc.).
- **Savings and investments were noted to face a threat** as:
  - Greater use of AISP and PISP services will increase transparency on rates and returns, while also offering easy ways to transfer.
  - Some are concerned that the use of 'money management' FinTechs could reduce the 'stickiness' of funds and introduce **greater volatility in deposits.** Taken to the extreme, this could impair the ability to lend due to liquidity coverage ratios and other regulatory requirements.
  - Cards networks (issuers, acquirers, merchants and schemes) are perceived to be threatened, primarily due to the **potential for PISP services to displace card transactions.** The rollout of 'instant payments' schemes across much of Europe is expected to intensify this threat.
- However, many noted that providing PISP and AISP services may create new revenue generation streams and/or attract new customers which may mitigate some of the impacts

What do you see as the greatest opportunity for your business arising from PSD2?



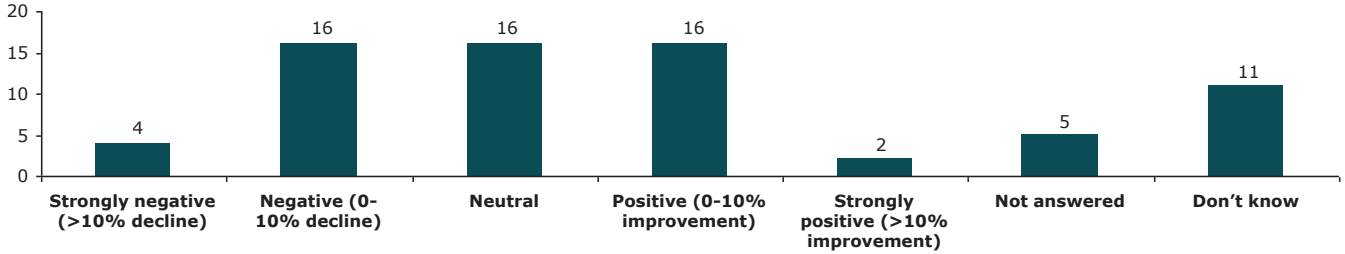
- The ability to better understand and serve customers through the increased access to customer data to was the major opportunity cited.
- Many believe PSD2 will allow a greater focus on customer needs, with some respondents considering how they can deliver products to the customer in the best way even if this is not through their own channels, opening up marketplace and distribution models.
- 21% of respondents believe PSD2 provides an opportunity for growth and/or increase in market share, as well as on opportunity to increase revenues and additional sources of revenues.
- However 13% of respondents do not currently see any major opportunities arising for their business, while another 4% are still considering the question.

Which type of market participant do you see as the largest threat to your organisation in relation to new services being introduced as a result of PSD2?



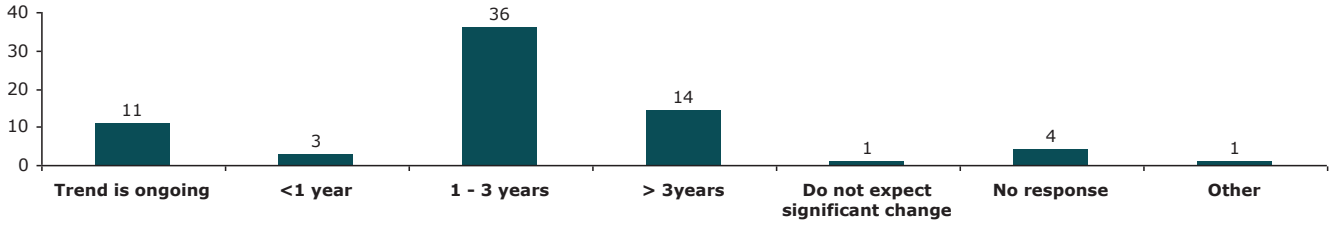
- The majority of respondents believe the **largest threat will arise from incumbent banks** (25%) and **"established" FinTechs** (21%).
- There appears to be a general sense that large existing incumbents are best positioned to respond, and most likely to gain from PSD2.
- Reasons put forward for this included:
  - They have the **financial resources** to be able to invest and to build compelling propositions.
  - They have the **internal capabilities** required to be able to develop such services, including specialist design and product functions.
  - Importantly, they have the **brand recognition** and trust. This is generally believed to be very important, at least until customers become more familiar with new types of services on offer.
  - They already have a **wide customer base** to leverage and from which to build.
  - They are more attractive partners to FinTechs and smaller organisations due to their scale, resources, brand and trust.
- It may be that rather than PSD2 increasing competition and facilitating new entrants as desired, the existing major organisations may actually capture and consolidate the market.
- However, **digital challenger banks came through quite strongly** (16%). This reflects the fact that such organisations do not have legacy IT systems to contend with and that this, coupled with more agile structures, allows them to adapt to the more quickly and efficiently.
- A significant minority of respondents saw the potential of **big Tech** companies to entering and disrupt the payments market being 'game changing' if unlikely.

What impact do you expect PSD2 to have on revenues and costs for your business?



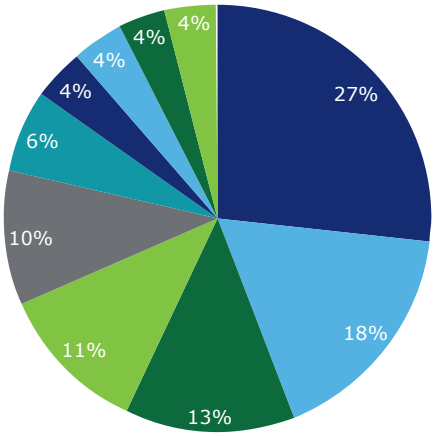
- The majority believe **PSD2 will result in significant competitive change over the next 2-3 years.**
- In terms of revenue and cost impacts, results were fairly evenly split, with roughly equal proportions expecting PSD2 to have a negative impact, a positive impact or a neutral impact in that order.
- Most respondents believe the **impacts will be relatively modest, especially in the early years of the implementation.** Very few respondents expect strongly positive or strongly negative impact.
- From a regional perspective, Central European respondents appear to be more pessimistic, while Western European respondents seem to have a more positive view.
- A substantial minority (16%) believe that PSD2 is not the driving force for any change, which is already ongoing, and that wider consumer demand for open banking will be the key determinant.

Over what period do you think PSD2 and Third Party Access will result in significant competitive change?



Final Thoughts

Other than 'Third Party Access to Accounts' and Strong Customer Authentication what do you see as the largest challenge in implementing PSD2?

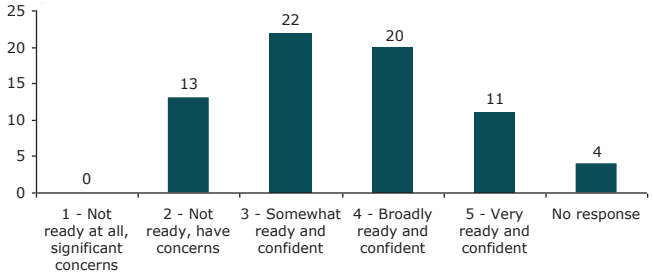


- Dealing with liabilities under the Third Party Access model, including investigation transactions and pursuing claims against TPPs
- Implementing new operational requirements such as new refundand unauthorized transaction investigation processes
- Risk Management and regulatory reporting
- Customer service, communications and complaints
- Uncertain regulatory requirements / lack of finalised RTS
- Extended scope for "one-leg" transactions
- Data management, protection and privacy, including tensions between PSD2 & GDPR
- Challenge to existing business model
- Limited resources
- Other

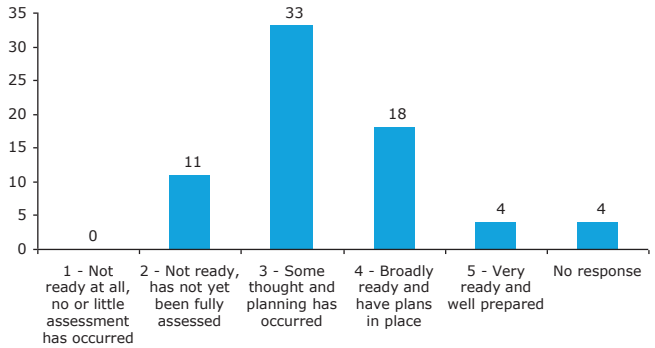
- As expected responses differ substantially, reflecting individual circumstances and models.
- The most common challenges reported were:
  - **Liabilities under the Third Party Access model** requiring the development of new models and processes for dealing with these issues, including how to investigate transactions made through TPPs, how to pursue claims against TPPs, and what to do in the event of disputes between ASPSPs and TPPs.
  - Challenges in implementing **new 'conduct of business' operational requirements** such as refunds, unauthorised transactions investigations and back-dating processes.
  - **Risk Management,** regulatory reporting and major incident reporting.
  - **Customer service,** communication and complaints
- 10% put the **lack of a finalised RTS** on Strong Customer Communications and Secure Communications at the top of their list of concerns.
- A further 3% also cited the difficulty in reconciling the 'tensions' between PSD2 and GDPR.

Readiness to respond

On a scale of 1-5 how do you estimate your organisation's readiness to comply with PSD2 by the implementation date?



On a scale of 1-5 how do you estimate your organisation's readiness to strategically respond to PSD2-enabled changes?



- The greatest number of respondents classed themselves as 'Somewhat ready and confident', followed closely by 'Broadly ready and confident'.
- This is encouraging as overall around 60% of respondents fall within these two categories.
- Only 16% organisations classed themselves as 'Very ready and confident'.
- Worrying, around 20% organisations classed themselves as 'Not ready, have concerns' suggesting a substantial proportion of the industry still has a significant amount of work to do.
- Almost half of respondents classed themselves as 'Some thought and planning has occurred'.
- Around 25% classed themselves as 'Broadly ready and have plans in place'.
- Whilst this is encouraging, this should be considered in the context of earlier responses; while many have begun the process for strategically responding to PSD2, the depth and extent this varies significantly.
- This can be seen most clearly in the small proportion of organisations (around 7%) classifying themselves as 'very ready and well prepared'.
- Just under 20% classed themselves as 'Not ready, has not yet been fully assessed'.

Contacts

EMEA payments leadership

Stephen Ley
Partner, UK
Risk Advisory
sley@deloitte.co.uk

Ian Foottit
Partner, UK
Consulting
ifoottit@deloitte.co.uk

Timo Span
Partner, Netherlands
Consulting
tspan@deloitte.nl

David Strachan
Partner, UK
Head of the EMEA Centre for Regulatory Strategy
dastrachan@deloitte.co.uk

PSD2 contacts by country

Kasper Peters
Partner, Belgium
Consulting
kapeters@deloitte.com

Petr Brich
Director, Central Europe
Consulting
pbrich@deloittece.com

Marko Hykkonen
Director, Finland
Consulting
marko.hykkonen@deloitte.fi

Marc Schmitt
Senior Manager, Germany
Consulting
maschmitt@deloitte.de

Adam Kissane
Senior Manager, Ireland
Consulting
akissane@deloitte.ie

David Mogini
Partner, Italy
Consulting
dmogini@deloitte.it

Roeland Assenberg van Eysden
Director, Netherlands
Consulting
rassenbergvaneysden@deloitte.nl

Phu Le Duong
Director, Norway/Sweden
Consulting
phduong@deloitte.no

Ana Seabra Brito
Senior Manager, Portugal
Consulting
anbrito@deloitte.pt

Gorka Briones
Partner, Spain
Consulting
gobriones@deloitte.es

Steven Bailey
Director, UK
Consulting
sjbailey@deloitte.co.uk

Andreas Lentzsch
Senior Manager, Switzerland
Consulting
alentzsch@deloitte.ch

Andrei Burz-Pinzaru
Partner, Romania
Reff & Associates - member of Deloitte Legal
aburzpinzaru@reff-associates.ro

Dimitrios Goranitis
Partner, Romania
Risk & Regulatory Advisory
digoranitis@deloittece.com

Authors

Adam Scott
Senior Manager, UK
Audit Advisory
adscott@deloitte.co.uk

Valeria Gallo
Manager, UK
Co EMEA Centre for Regulatory Strategy
vgallo@deloitte.co.uk

Deloitte.