INNOPAY

Book of Insights 2020

#EverythingTransaction

innopay.com

Table of Contents

Foreword

Shikko Nijland
is co-owner and
managing partner
of INNOPAY

GET IN TOUCH

At INNOPAY we believe that everything is becoming a digital transaction, because all underlying and derived data represents economic value. We regard this as the transactional phase of the internet, with as-yet-untapped potential of Blue Ocean value driven by the exponential growth of digital transactions. The pace and magnitude of change is so great, however, that by the time you realise the true implications for your organisation, it may be too late to act. In the worst-case scenario, your entire industry will be disrupted.

Of course, most organisations know this and are already rethinking their position in this new data-driven world of real-time, many-to-many connectivity. To help leaders to focus on staying relevant, we have put together this compendium of recent blogs written by our experts. The main common threads running through them are digitisation, data sharing & data sovereignty, and collaboration.

We have almost 20 years' experience of helping organisations to create a collaborative advantage. In fact, we've developed our own flexible and proven co-creation process that blends business, technology and regulatory expertise to deliver new added value. We hope that this collection of blogs will help you to find new inspiration for dialogue, collaboration and innovation, not only within your own organisation but also within the wider ecosystem. Please feel free to contact us with any comments, suggestions or inspirational ideas relating to the topics covered here. We're always happy to hear from you!

Shikko Nijland

INNOPAY

BLOG

Digitising complex onboarding processes: Who will be leading in getting it right?

26 December 2019

Josje Fiolet

Guy Rutten

GET IN TOUCH

INNOPAY

In the past year, customer onboarding processes for simple financial products have become much more convenient. The INNOPAY Onboarding Benchmark (2018) shows that almost all Dutch banks now have a customer friendly, digital onboarding process for opening a payment account, inspired by the challengers like Revolut, N26, and Monzo offer across Europe. Thinking about how much the market has changed in the past year, it is only a matter of time before onboarding of more complex products will be digitised as well. So the question is: who will be leading in getting it right, banks or fintech?

For more complex products the onboarding process is still very complex and cumbersome, as non-digital steps are involved. Complex products have stricter regulatory and risk requirements – and with AMLD4 set into national law in 2018 and AMLD5 already coming up, no leniency is expected any time soon. Regulation is often seen as an impediment to customer facing innovation and perceived as a trade-off for user experience. At INNOPAY we see this differently. Existing technologies can both enhance the customer experience and improve the security of the onboarding process.

For banks, it is time to approach onboarding from this perspective. First, because consumers expect a fast and fully digital experience. In a commoditised business-like transactions this is becoming the differentiating experience. Second, because compliance cost for both implementation and accuracy will rise if manual operations

are maintained. People checking documents and re-entering data are both expensive as well as error prone. It is expected that digital challengers will change the onboarding landscape for complex products in the same way they did for the "simple" products. However, established players still manage to keep challengers at length, as they have the advantage of a large and typically loyal customer. But for how long? Let's talk about what is needed to keep it that way.

1. From risk at the product level, to risk at the customer level

Obviously, not all customers are the same and therefore the risk profile differs per customer. Banks, however, are used to determine the risk involved at product level measuring every customer against the same stick. The onboarding process for complex products has become unnecessarily difficult for most customers, having a negative impact on the user experience and conversion ratios. Furthermore, the process forces banks to put the same effort in the low as well as the higher customer risk profiles in terms of data gathering, file creation and monitoring. A personalised process can save time and cost for both the customer and the bank.

2. Modular onboarding building blocks

Onboarding processes preferably cater for a variety of contexts, as explained above. Modular building blocks form the basis for processes that serve different products, customers and channels. The onboarding process can be designed with different sets of building blocks, which might vary given the specific relevant context. The required level of compliance and the risk involved can be used to determine which building blocks apply for a specific situation.

Within the different building blocks, new technologies can and should be used to add both security and convenience for the customer and bank. Innovative technologies are often perceived as risky due to lack of experience and best practices. Fortunately, the European Supervisory Authorities (ESAs) are helping out. They published a guideline with questions that help banks assess if an innovative solution is fit for purpose. In short, ESA's guidance determines not if, but how new technology can be used to optimise a building block.

3. Start small with the end in mind

So, how to design and implement a more personalised and modular process, using technology in a controlled manner, as described by the ESAs? Improving the onboarding process is quite complex as it touches upon so many systems and departments. A good start is to describe the ideal process. After setting the end goal, the process should be split up in building blocks that can be optimised separately. This enables banks to focus on operational effort per building block, rather than having to change everything at once.

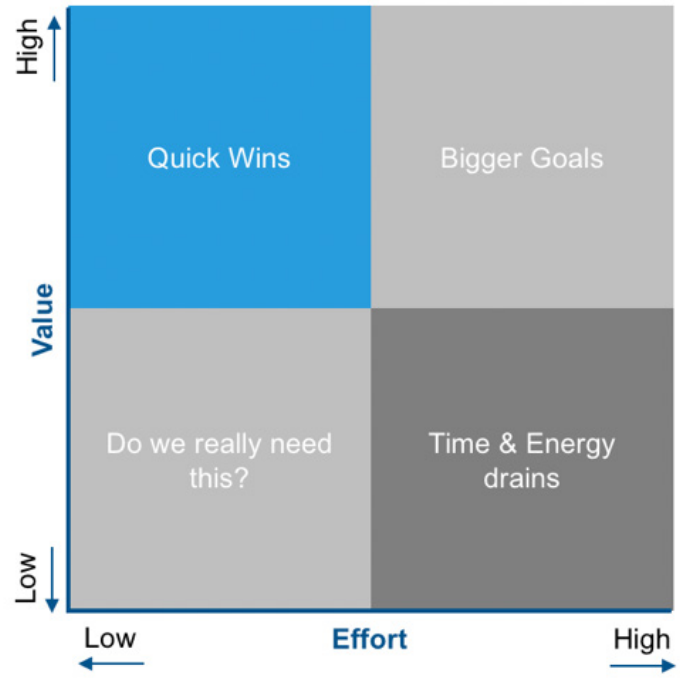


Figure 1: Effort x Value matrix to prioritise activities

To prioritise initiatives, the simple yet effective "Effort x Value matrix" can be used. The focus should be on the Quick Wins. "Quick Wins" are improvements that require relatively little implementation effort and have a big impact on the value created. Examples are improvements in user experience like automated document read and reduced number of required data fields. Not only will the customer experience improve as straight-through processing ratios will increase, but also data quality will improve, enabling banks to enhance decision making on how to best monitor customers going forward.

The Quick Wins can only be derived from picturing the "Bigger Goals". Working incrementally will lead to quicker results, a steeper learning curve, easier buy-in of internal stakeholders, and most importantly, it shows the customer you are taking them seriously by continuously improving the journey.

To conclude, a step by step approach, using new available technologies in a modular way, can help financial institutions to digitise more complex products, make processes more secure, and most important, keep their customers satisfied and loyal in return. So maybe this time the banks will lead the way!

Authors

Josje Fiolet and Guy Rutten

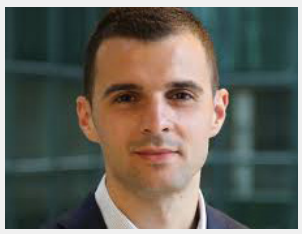
ORIGINAL BLOG

GET IN TOUCH

BLOG

Open Banking Monitor 2019: let's take a moment to make up the rankings and identify potential new "Masters in Openness"

23 January 2019



Mounaim Cortet

Art Stevens

GET IN TOUCH

INNOPAY

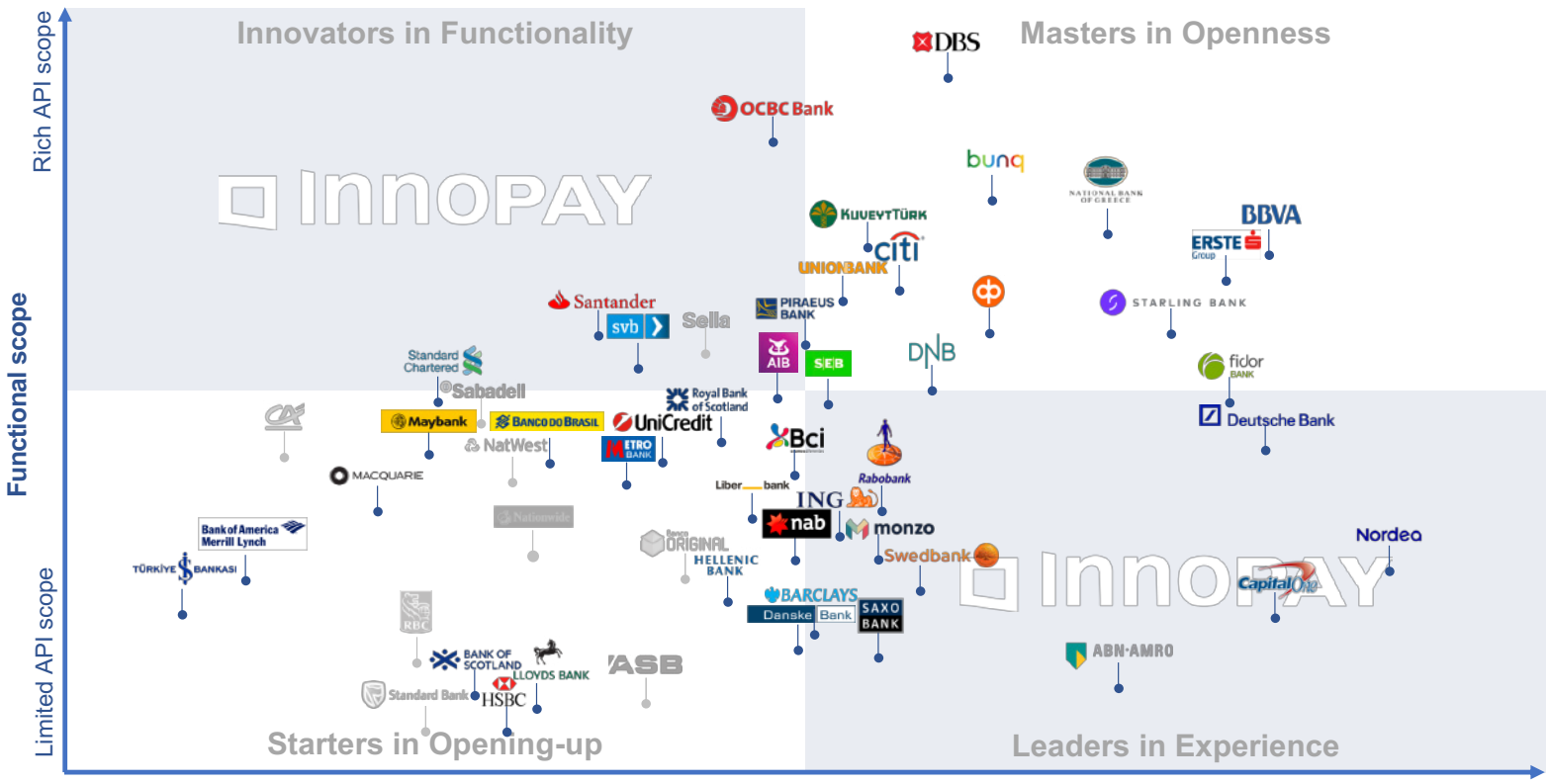
Looking back on a much eventful year in Open Banking; various banks have updated their Developer Portal in the last quarter of 2018, either by expanding the Functional Scope, by offering more APIs, or by introducing tools and features improving the Developer Experience. Predominantly with the shared goal of attracting more end-customers, better servicing developers to work with the bank's APIs and strengthening their overall position in the Open Banking landscape.

For some banks, however, when it comes to Open Banking, stagnation also means decline, as other banks are not resting on their laurels. New functionalities and (extension of) developer tools continue to be added by the 'Masters', whereas other banks are struggling to keep up that much desired pace. Slowly, but surely banks develop the required capabilities to excel in Open Banking, with many banks learning from each other's releases to shape their own journey.

Compelling developments through creative api design and introduction of co-creation

OCBC and Capital One have put great effort to update their Developer Portal. Where OCBC has added several functionalities in the area of account data and customer functions, they've also introduced some new unique features, such as "Request credit limit increase API" (i.e. an API for requesting a credit limit increase) and "Off-boarding API" (i.e. deregistration of a corporate bank account from the account repository). Capital One has improved on Functional Scope and Developer Experience and seems to be heading towards a collaborative API marketplace. Capital One provides articles from (external) Open Banking experts and developers to collaboratively introduce app ideas and offer hands-on use-cases of APIs. This will most likely lead to easier idea generation and will guide the developer further towards consuming the

that it is a person and not e.g. a picture). NBG also offers a "Crowdfunding API" letting third parties integrate their crowdfunding application with NBG's digital channels. This lets (smaller) third parties benefit by collaboration with a crowdfunding platform. Kuveyt Turk, as a newcomer to the OBM, offers besides a wide range of APIs also an "Incident Operations API", where incidents can be created and managed. Nordea has introduced an "Instant Reporting API", increasing the value of account data functionalities by providing real-time account information. ERSTE Group has done a great update on their sandbox extending many functionalities we haven't seen before (e.g. variances in required authentication, user friendly example values, easy switch to production data etc). This makes the testing environment very developer friendly!



*Grey indicates limited portal accessibility, thereby complicating full assessment

INNOPAY *Open Banking Monitor (OBM) – Developer Portal benchmark (update January 2019)*
Note: If your bank is not in the OBM yet, go to openbankingmonitor.com and let us know!

Capital One APIs. Capital One has also made additions for their identity API, besides federated login, they offer three variances 'Sign up', 'Sign in' and 'Verify ID', letting other parties use the verified identity of Capital One users.

The National Bank of Greece (NBG) introduced a "Biometrics API", for comparison of faces in images and also check the actual liveliness of a person in a video (i.e. making sure

Welcoming new banks to the open banking landscape

Piraeus, Den Norske Bank, Nationwide, Kuveyt Turk and Liberbank have been added since the last release of the OBM in September 2018. From a Developer Experience perspective, it is worth mentioning the different approaches to handling and making available the API Documentation. Whereas Nationwide is offering their full API Documentation (based on UK Open Banking [1]) by including a link to the Open Banking

website, Den Norske Bank is offering their API Documentation by using ReDoc, i.e. an open source swagger generated API reference documentation. As discussed in the previous release of the OBM, ReDoc might be a solution to start with standardisation of the Developer Experience components, in this particular case API Documentation.

Conclusion

The Open Banking landscape continues to evolve, as evidenced by the developments since our last update around three months ago. Various new ideas and APIs have been introduced, also as a result of collaboration between banks and third parties. The clarity and similarity of functionalities and tools shows that banks are increasingly learning from each other, strengthening the cohesion between banks and third parties. This will likely result in some exciting developments in the Open Banking landscape in the course of 2019 that we will capture in our periodic OBM releases. Stay tuned for more updates!

Other updated developer portals: Starling, SVB, Deutsche, Bunq, Swedbank, Allied Irish Bank, Standard Chartered.
Banks with limited or no accessibility of their developer portal: CA, Sabadell, Royal Bank of Canada, ASB, Natwest, Standard Bank, Original Bank, Banca Sella, Nationwide, Wells Fargo, JP Morgan.

1. UK Open Banking - https://www.openbanking.org.uk/

Authors

Mounaim Cortet and Art Stevens

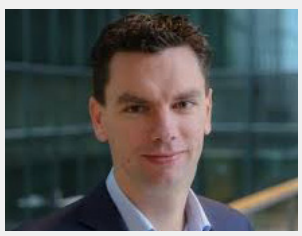
ORIGINAL BLOG

GET IN TOUCH

BLOG

Is “Open Insurance” the next Uber of the industry?

4 February 2019



Maarten Bakker

Vincent de Rijke

GET IN TOUCH

INNOPAY

As every interaction becomes a transaction, Open Insurance or API (B2B2C) insurance is being labelled to bank in on this trend. Although that sounds amazing, the term still lacks a good definition to provide meaningful guidance for insurance companies. To get more clarity INNOPAY has defined 7 Open Insurance roles for the industry. Insurers should take notice and make a clear positioning choice to enable new revenue and business models whilst ensuring continued relevance and growth.

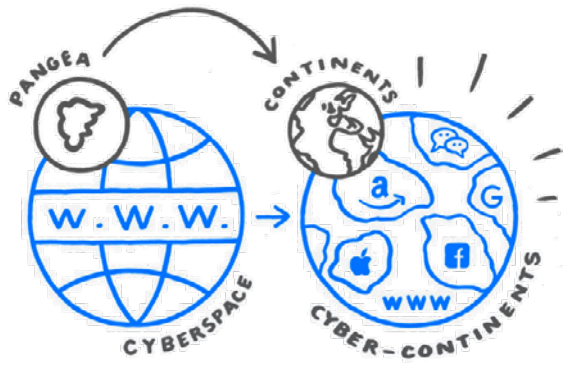
Uber model for insurance? Not so fast

Insurers know how Florida residents are feeling. The pressure the industry is facing seems to keep coming like an unending stream of hurricanes: continuous digitalisation of processes, the rise of online aggregators, rising customer expectations (millennials & Gen Z), a continuous focus on new regulation and compliance, low interest environments, modest to low economic growth and disruption of the value chain by InsurTechs.

In this environment change is hard, and the statement is often made that it is only a matter of time before a new Uber like player will disrupt the industry. Of course, this comparison does not hold. Not in the least because of the low consumer interest in these products but also because in a networked model there is not an increasing need to transfer risk and thus grow the core insurance market. Whereas an increasing use of for example AirBnB by both hosts and customers leads to network effects of new hosts and new customers.

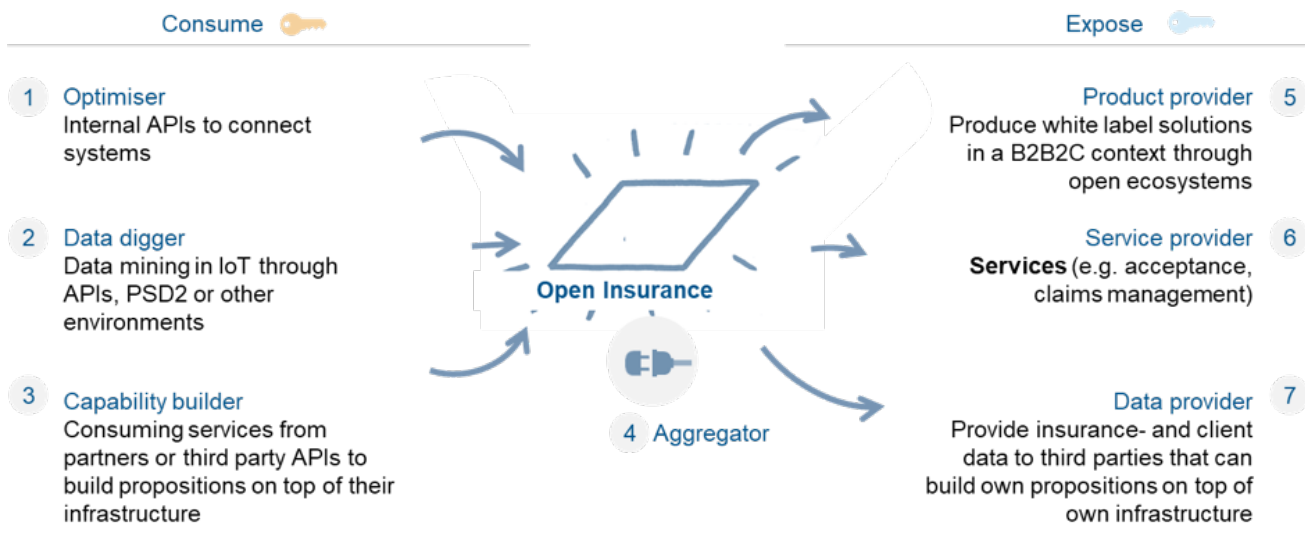
But then what? 7 Open insurance roles to structure the world

That said, platforms are rising and eating the world.
And InsurTechs are developing new propositions which are replacing parts of the traditional value chains of insurance



companies. To stay relevant and bank in on the position of networked platform players insurers need to open up. Openness is about getting access to increasing and vast amounts of structured data in many-to-many situations to enable new open ecosystem propositions. Basically, this is nothing new as there are numerous examples of industry or commercial initiatives which are driving this trend.
Think about sharing fraud detection signals via shared databases or commercial parties. But the trend towards openness is becoming more and more important as digital transactions are growing exponentially [1].

This trend towards openness by the industry is often labelled as "Open Insurance" which is a term rising because of the Open Banking trend. But whereas Open Banking seems to be a (somewhat) settled definition this is still not the case with Open Insurance. Initiatives like the Open Cologne [2] or the Open Insurance Initiative Network (OPIN) [3] work towards API standardisation for (consumer) data sharing in combination with consent. To get more clarity INNOPAY has defined 7 Open Insurance roles for insurance companies.



1. Optimizer

Insurers are often very siloed organisations. To enable cross-product and cross-channel offerings, insurers are working on data standardisation, governance and stewardship in combination with internal APIs to facilitate meaningful data sharing.

Example: an internal optimisation we have seen at one Dutch insurance company using an API interface to couple their policy administration systems, client request database, and payment software in order to increase the operational excellence, decrease throughput times and handling time per request, driving down operational costs while increasing customer satisfaction.

2. Data digger

One of the most promising trends for insurance companies is the exponential growth of structured data which can be consumed and used with customer consent. This data can be used to enrich product or service offerings, more targeted customer propositions or better risk management.

Example: PSD2 is of course a huge opportunity for insurers [4] but also social, IoT [5] or other platform sources can be very relevant. Using external and personal customer data enables insurers to increase the accuracy of actuary risk models.
One step further, using real-time customer data (e.g. connected car) input enables insurers to provide insurance with dynamic risk models – and pricing. This enables insurers to attract target groups with a more diversified or personalised product portfolio.

3. Capability builder

Building upon available services through API's increases insurance capabilities, enriching the services for customers. Insurers can, for instance, improve their selling process by using one or more third party services for customer plans.

Example: Access the customer Gmail API to get email information about planned trips based on airline or hotel booking confirmations. Based on this information the experience around travel insurance can be enhanced.

4. Aggregators or schemes

Develop a platform where many-to-many API connections are facilitated by offering standardized connections. In a landscape with many different API developers, providers, platforms and insurers -each dependent on an until now non-standardised API landscape- the party that is able to aggregate API's and becomes the standard go-to marketplace for data and services, is in the leading position to learn from data capabilities and monetise the aggregator model once it has become the industry standard.

Example: Price aggregators have already become very common but other aggregators or schemes could take off when new structured data sources become accessible.

5. Product provider

Insurers that can develop relevant and user-friendly API's can decrease their dependence on brand value. Using API's, insurers can provide white label products in a B2B2C model in an open ecosystem. This, just like insurers that can provide (partial) services, means increased revenue when other insurers or commercial parties offer their network of customers your insurance products, be it white-label or not. Insurers mastering this process can increase conversion without marketing, sales because of integration into processes previously hardly accessible, and increase scale of their insurance portfolio.

Example: Lemonade and Simplesurance are offering API's to 3rd parties to integrate their products in their customer journeys.

6. Service provider

Insurers able to leverage on their core capabilities by providing services or partial services through API's, (e.g. claim handling, fraud reduction, policy acceptance), can increase the revenue by exposing core capabilities, or by ways of becoming a shared service centre. This is especially attractive for insurers where operational scale is of utmost importance to remain profitable.

Example: insurers can monetize on their fraud detection algorithms and expose them to 3rd parties.

7. Data provider

Insurers that leverage their existing customer relations and build on the trust that customers have in the company can increase customer relevance or increase monetisation models through exposing insurance and client data– with consent - to third parties so these third parties can build or improve services upon this data.

Example: insurers have insight in customers, with which they can expose and monetise their accurate customer persona, policy details, claims data to other commercial parties where customers have (potential) business.

So, how to bank in on openness?

There are several questions coming into play for insurers when considering becoming a trusted player in open ecosystems.

- How can openness increase relevance to our customers?
- How does openness impact our strategy and business model?
- Which open insurance roles are suitable to execute on?
- Which data and capabilities do we need to leverage internally?
- How do we structure and monetize our API's to new and often unknown ecosystem players?
- How can we partner with the InsurTech scene?
- What can we learn from banks and other parties connecting to their ecosystems and building new open business models?
- How can we attract the right talent to deliver on these new opportunities?

Before insurance companies move forward and invest in programs to become the next Uber, they have to ask these questions. Providing clear answers will help them navigating the challenges ahead and make sure their investments are worthwhile. Want to discuss, please reach out to Maarten Bakker or Vincent de Rijke.

1. https://www.everythingtransaction.com/

2. http://deliverythinking.com/open-cologne-the-first-open-insurance-initiative/

3. https://openinsurance.io/

4. https://www.innopay.com/en/publications/insurance-and-open-banking-wave-seven-use-cases

5. https://www.innopay.com/blog/how-openness-will-change-insurers-pricing-strategies/

Authors

Maarten Bakker and Vincent de Rijke

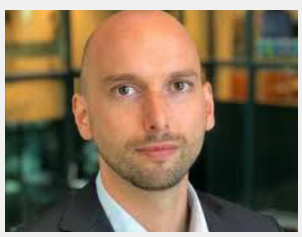
ORIGINAL BLOG

GET IN TOUCH

BLOG

PSD2 licensing: solving the puzzle of becoming a Third Party Provider

21 February 2019



Tycho van Ewijk

Josje Fiolet

GET IN TOUCH

The European Union (EU) revised Payment Services Directive (PSD2) was adopted January 2016 as an update of PSD 1 (adopted in 2007) and introduces two types of new services under its licensing scope: payment initiation services and account information services. New players in the financial industry and incumbents (e.g. banks, electronic money institutions) that intend to offer these services will be referred to hereafter as Third Party Providers (TPPs). In a series of upcoming blogs, we will elaborate further on the key opportunities and challenges for TPPs.

Being or becoming a TPP opens up business opportunities for incumbents and new players alike but requires careful consideration of the cost of compliance, which arise from acquiring the license but even more so from maintaining it. These costs can be optimised through a proper implementation of the PSD2 licensing requirements, which have a broad organisational impact in areas such as business operations, risk management, compliance, governance, and reporting.

This first in a series of blogs aims to help potential TPPs with understanding the regulatory requirements and to successfully acquire and retain their licence in a strategic and efficient manner. We focus on PSD2, but please note that being a licensed business also entails complying with other regulations such as GDPR, AMLD and eIDAS.

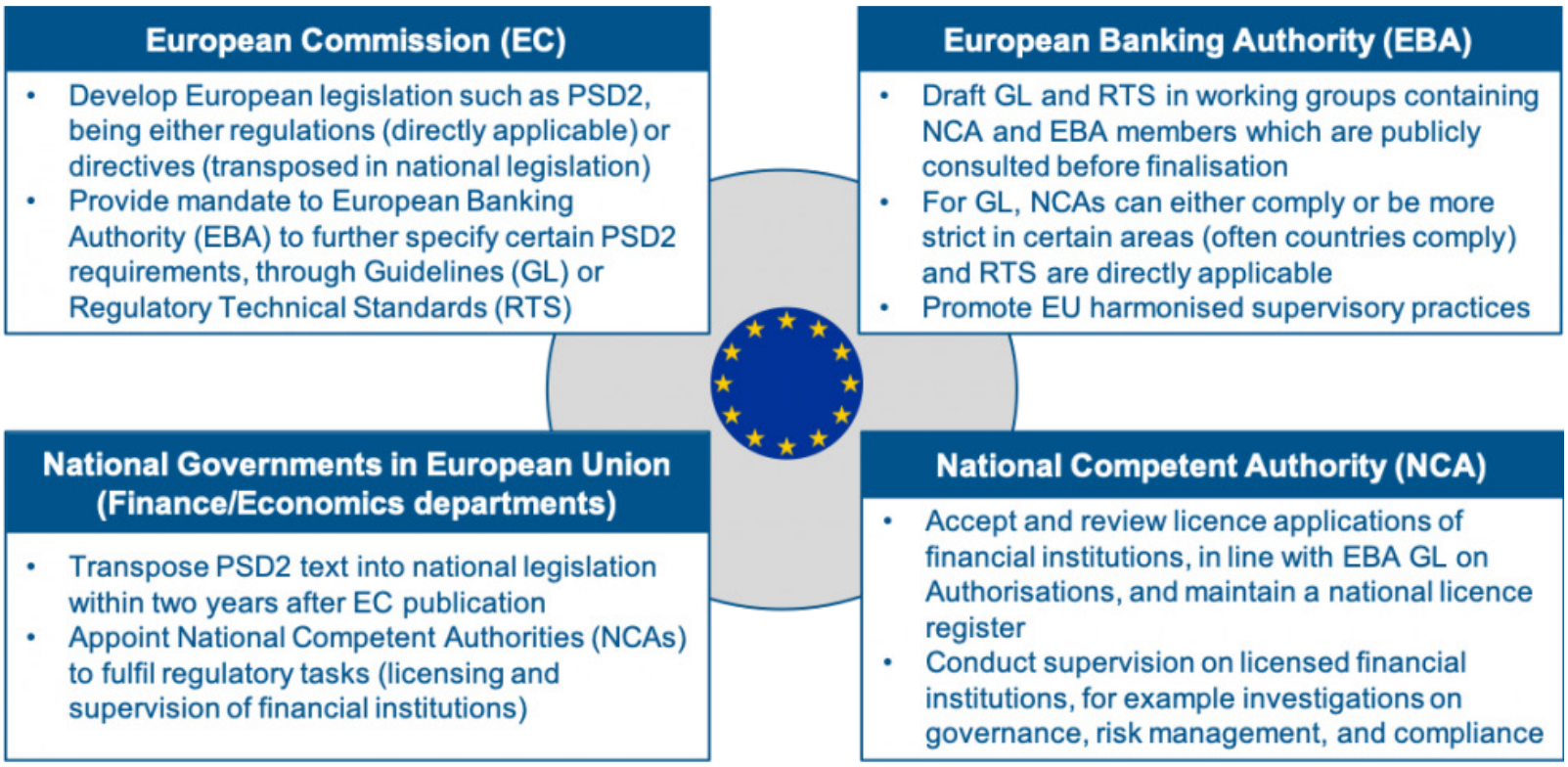


Figure 1. Simplified overview of the main stakeholders within the European Union regarding PSD2 . © INNOPAY BV. All rights reserved.

Overview of the PSD2 regulatory landscape

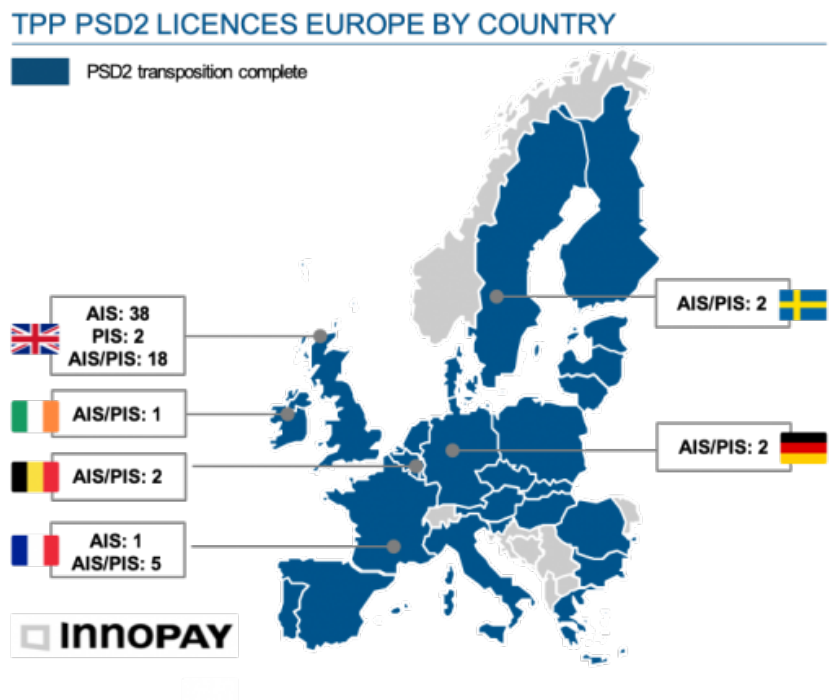
A lot has been said and written on PSD2, often leading to misinterpretations of the timelines and requirements of becoming a TPP. Forget all the confusion as we provide you with a clear view on the most relevant topics.

The picture below provides a (simplified) overview of the four key stakeholders within the EU who are involved with the design and implementation of the PSD2 rules.

Due to the sheer amount and complexity of the regulations, various EBA GL and RTS experienced delays and several EU countries (e.g. Belgium, Netherlands, Spain) missed the transposition deadline of 13 January 2018. Main reasons were conflicts of interests between TPPs and Account Servicing Payment Service Providers (ASPSPs, being mostly banks) and discussions on sensitive topics such as privacy aspects in relation to processing payments data. The effect of these delays and complexity is seen in the limited amount of TPP licences issued in the EU, which is displayed in Figure 2.

We expect TPP licensing activity to increase now that the dust has settled and most regulatory requirements are known, and we will continue to monitor this.

In total, 14 documents have been published by the EBA, which are described below and ranked by relevance to TPP licensing. A good understanding by TPPs on the impact of the standards and guidelines on their organisation contributes to a more efficient licensing process.



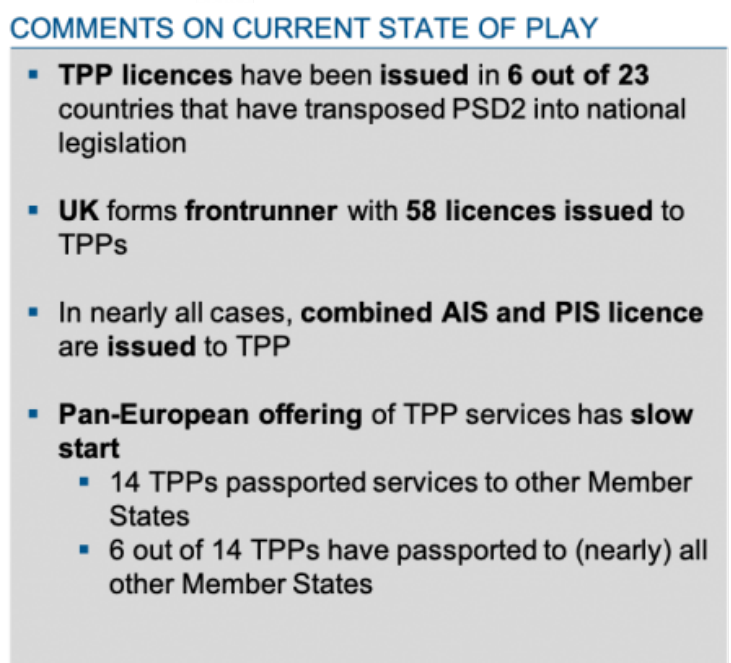


Figure 2. INNOPAY TPP Radar (update January 2019). © INNOPAY BV. All rights reserved.

#	EBA publications on PSD2	INNOPAY indication of relevance for TPPs
1	GL on Authorization of Payment Institutions	**High.** Describes the minimum licence requirements for TPPs (who need a payment institution licence or registration to operate) which are taken into account by the supervisor
2	GL on Operational and Security Measures	**High.** Contains strict requirements on governance, risk management and assessments, monitoring, testing, and business continuity (note: soon replaced by GL on ICT & security risk management)
3	RTS on Strong Customer Authentication & Common and Secure Communication (SCA & CSC)	**High.** Technical standards on TPP interaction with banks such as security measures, strong customer authentication and communication, applicable per 14 September 2019 (note: parts of this RTS are further detailed in documents #7, #9, and #10 in response to market concerns)
4	GL on Fraud Reporting	**High.** Reporting requirements on payment/fraud data, only for TPPs who initiate payments
5	GL on Incident Reporting	**Medium.** Details criteria, thresholds and method to be used for incident reporting to supervisors
6	GL on Professional Indemnity Insurance	**Medium.** A TPP insurance or a comparable guarantee is a prerequisite to be granted authorisation
7	Opinion on the implementation of the RTS on SCA & CSC	**Medium.** Provides clarity on the exemptions to SCAs, consent, data sharing scope, and the requirements for banks to provide dedicated interfaces and contingency measures
8	RTS on Passporting	**Medium.** For the international provision of payment services (by TPPs) in the EU
9	GL on the contingency mechanism exemption under the RTS on SCA & CSC	**Medium.** Provides clarity to banks and supervisors regarding the elements to be considered for the exemption process for providing a contingency (i.e. fall-back) interface, incl. interaction with TPPs
10	Opinion on the use of eIDAS certificates under the RTS on SCA & CSC	**Medium.** Clarifies on TPP identification by banks: use of qualified certificates for electronic seals (QSealCs) and qualified certificates for website authentication (QWACs)
11	RTS on EBA Register	**Low.** A central register will contain TPP licence information used by banks to grant TPPs access
12	RTS on Central Contact Points	**Low.** Supports host supervisors with contacting foreign TPPs that operate within their jurisdiction
13	RTS on Home Host Coordination	**Low.** Aimed at national supervisors, but may lead to local reporting requirements for foreign TPPs
14	GL on Complaint Procedures by CAs	**Low.** Complaint procedures for payment service users for alleged infringements of PSD2

Figure 3. INNOPAY indication of TPP relevance of EBA GL, RTS, Opinion publications under PSD2.

We advise potential TPPs to first assess the requirements in the documents with high relevance and work their way down to the medium/low relevance documents. The regulatory assessment results provide valuable input to the development of your business case which is a vital step to complete before a licence application should take place.

Business case development

Acquiring and retaining a licence in the financial sector has proven to be challenging for organisations. This can result in long application processes (easily lasting longer than 9 months), supervisory fines and unforeseen required operational changes. These negative experiences cultivate an often-expressed view on licensing and supervision as being a 'regulatory burden' with high costs. The PSD2 regulatory framework poses similar challenges, looking at the sheer number and impact of the requirements, but if done right it can be far less costly to acquire and retain a licence. We have also seen cases where a licence trajectory had an overall positive, indirect cost impact since it forced the respective business to streamline and 'declutter' operations and enhance the overall business.

Development of a solid business case should assess the opportunities and costs at least on the following three levels: strategic (e.g. products, competition, market), regulatory (e.g. gap analysis) and organisation (e.g. operational readiness). Doing this properly will get TPPs off to a good start of the licence application process, which is further described below.

The licence application process and beyond

The PSD2 licence requirements cover topics such as a payment services description, business plan, governance arrangements, management suitability, internal control framework, risk management and compliance, security and operational standards. The main purpose of the supervisor is to gain confidence that the TPP is running a professional business in all these areas and follows the relevant rules. We suggest TPPs take a structured and tailored approach towards their licence applications which covers the full licensing life cycle (see Figure 4 below). In our next blog we will further detail the phases and pay extra attention to the essential role of shaping the operating model in an activity-based manner from the start.

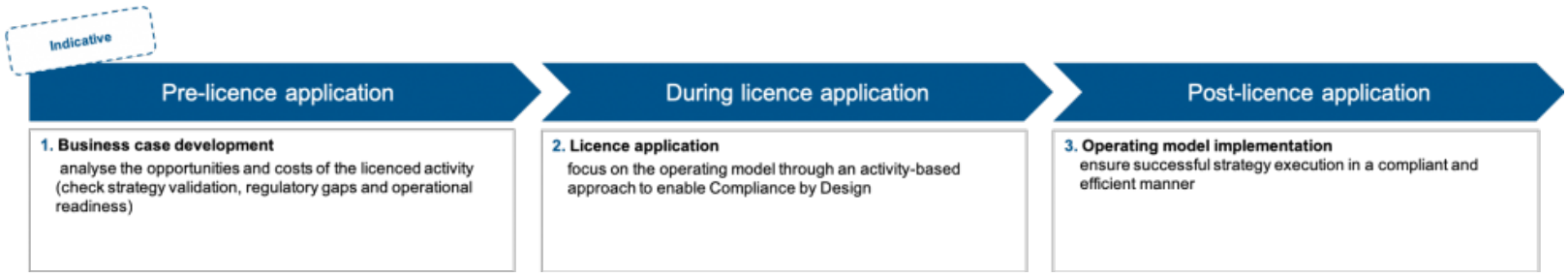


Figure 4. Indicative structured approach towards licensing based on INNOPAY analysis.

The overarching idea is to map the regulatory requirements to the current operating model and create a plan to address any gaps, whilst taking into account supervisory guidance and best practices. For the licence application it suffices in most areas to submit documentation showing a compliant organisational set-up (as the licensed products have not been launched yet). Basically, this entails drafting and submitting documentation such as policies, procedures, and risk assessments. But in order to retain the licence and operate without raising supervisory concerns (which are often accompanied by mandatory repairs), TPPs need to be able to demonstrate a compliant way of working to the supervisor. This is why TPPs are wise to start (re) designing their operating model early in the licence application process to ensure 'Compliance by Design' for their activities and avoid future costs.

In our experience, implementation of a compliant way of working is most challenging for the requirements in the following areas:

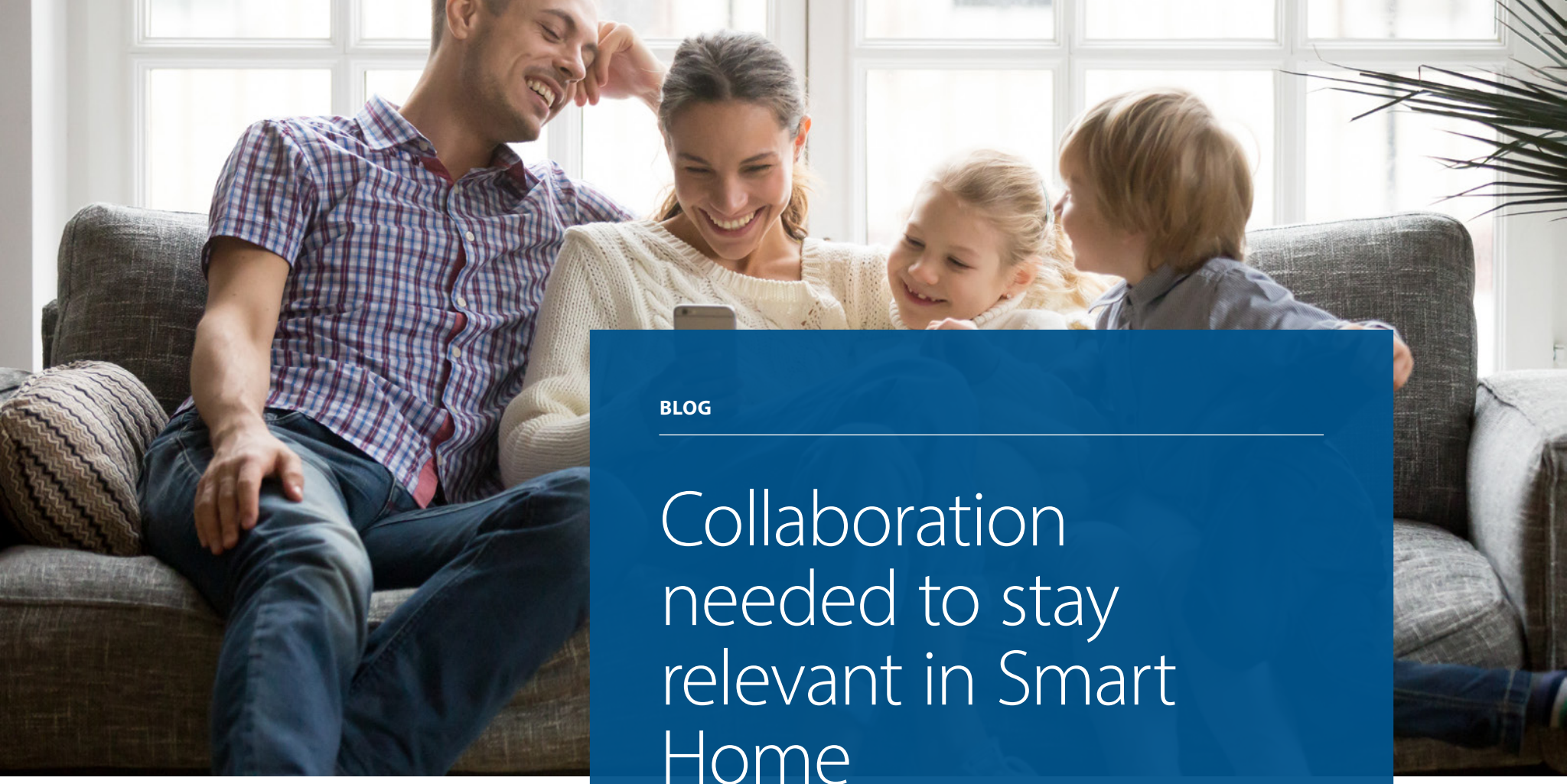
- Operational and security risk management framework, with detailed and high impact requirements on incidents, fraud, authentication and communication
- Anti-money laundering and combating financing of terrorism and especially requirements on Customer Due Diligence (Know-Your-Customer principles) and client/ transaction monitoring
- Governance and especially the requirements of a proper segregation of duties (first, second, and occasionally third line of defence)

If you want to start your (pre-)licensing process today, just reach out to Josje Fiolet or Tycho van Ewijk to discover where we can help you. Also, look out for our future blogs where we will dive deeper into these specific licence requirements and how Compliance by Design can be ensured.

Authors
Tycho van Ewijk and Josje Fiolet

ORIGINAL BLOG

GET IN TOUCH



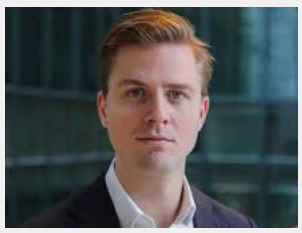
BLOG

Collaboration needed to stay relevant in Smart Home

3 April 2019

Esther Groen

Denise Hoppenbrouwer



Jim de Wolf

GET IN TOUCH

With the rise of the Internet of Things (IoT) and artificial intelligence (AI), transactions initiated by smart devices and platforms will increase exponentially over the next years. An appealing example is Smart Home, which connects customers digitally through smart devices and allows them to share data and transact from home 24/7. As research shows that already 33% of the Dutch population expects to start purchasing products and services via Smart Home devices within five years, we believe this is the next level commerce.

In such a "connected" environment, customers behave differently compared to the traditional on- and offline channels. Not only customers, but also platforms or devices will buy and pay for products and services applying smart algorithms to data gathered. This will particularly impact retailers, but also affect producers and payment service providers (PSP).

For the sixth year in a row, INNOPAY has contributed to the ShoppingTomorrow research program. Together with equensWorldline we hosted the expert group 'Payments in Smart Home'. In this collaborative project a group of experts researched the effects of Smart Home on Retailers, Producers and Payment Service Providers. This blog provides the main insights of this project.

In Smart Home, visibility to the customer decreases, the competitive landscape shifts due to new competitors and current propositions and business models no longer suffice to support and deliver a 'connected' customer journey. Time to start acting, do things differently and seek for new collaborative ways to address these challenges and leverage the opportunities that come with Smart Home.

Smart home significantly impacts visibility to customers

Retailers struggle with the growing popularity of Smart Home. Where they are now the main purchasing channel for customers, in Smart Home their position is very likely to be disintermediated by platforms and devices.

In Smart Home or a 'connected' environment, platforms and/or smart devices determine on behalf of customers what products or services are offered. With IoT and AI personal data is gathered and analysed to proactively anticipate on customers' needs. As the concentration curve of customers in Smart Home shortens – it has to be instant and personalized - the number of offerings is limited to roughly three out of the current ten offered online*. As a consequence, the visibility of retailers not only depends on the Smart Home platform or device, it is also crucial to make sure their products or services are included in the Smart Home spot list offering.

Further complicating the matter, the spot list will be shared with new competitors; producers and tech-giants. In Smart Home producers are offered the opportunity to envelop the retailer and directly offer their products and services to customers via Smart Home. Additionally, tech-giants like Amazon and Google, are also moving up the value chain using their own platforms (e.g. Alexa and Google Home) to sell their products. So, disintermediation of retailers, decrease of available spots, and new competition significantly impacts the visibility to customers.

Propositions no longer suffice in the smart home context

Smart Home is all about offering instant tailor-made convenience to customers, resulting in a different customer journey. An ideal Smart Home proposition offers an end-2-end seamless customer experience from orientation to delivery, integrating the purchase and payment journey. Smart Home platforms and devices primarily aim to take over customer orientation by using for instance AI and voice. They identify awareness, offer personalized offerings and finally help customers choose and pay for the product or service in a seamless way. Current Smart Home offerings, however, are still fragmented, lack interoperability and focus primarily on the purchasing journey.

To stay visible and relevant, it is pivotal for retailers and producers to 'merge' their propositions with Smart Home. To become visible in Smart Home via an existing platform both retailer and producer need to pursue a competitive pricing and/or distinguishing branding strategy. A producer with a strong brand or a retailer with the best pricing is more likely to be selected by the platform as conversion rates are higher. To become relevant in Smart Home, propositions need to integrate the full customer journey. We already see examples where retailers collaborate with suppliers and service providers to offer a 'device and delivery integrated' offering (e.g. smart lock for delivery groceries based on customer consent[1]) or experiment with voice to increase convenience.

The payment experience is an important element to further improve convenience. A good example is Uber, who has seamlessly integrated the payment into the purchasing journey. In Smart Home, customers expect a similar experience. However, in Smart Home different customer profiles, products and services come together and the range of payment methods offered expands. Interoperability and ease of use will be key. Groceries for example are often paid post or at-delivery via an instant payment, whereas an insurance service product can be a mix of pre-payment (direct debit) for basic insurance needs and pay-per-use (instant payment) for occasional insurance needs (e.g travel insurance). During onboarding the customer will select their preferred payment method per product or service, which in all subsequent transactions merges with purchasing journey save for the authorization of the payment. For merchants it is important to incorporate these payment requirements into their propositions. For PSPs it is an opportunity to increase their relevance for merchants and offer an integrated wallet offering and onboarding services to both meet the needs of merchants and the Smart Home customer. In short, propositions will need to be adjusted to the Smart Home context and on top create an end-2-end seamless customer experience through collaboration.

Adapting business and operating model to smart home

Finally, it will be difficult for retailers to maintain their pole position as purchasing channel in Smart Home. Retailers will have to change their business and operating models to create relevance in different parts of the value chain. Some supermarkets are already rebranding stores to 'experience and fulfillment' centres to influence customer preferences. They aim to surpass the Smart Home algorithms that have a tendency of locking in customers and not offer them "new" experiences. Other retailers are for instance differentiating to offering last-mile delivery services and create new customer touch points in the Smart Home journey.

For producers, the impact of Smart Home on their business and operating model is significantly smaller as they 'simply' can replace current retail channels and distribute their products and services via the Smart Home platforms. However, increased competition and deviating customer orientation, forces them to use pricing and branding as dominant unique selling points.

Smart Home is still very much a fragmented environment and as such PSPs have a role to play. It is more than ever essential for PSPs to create scale on the one hand and offer tailor made payment services that meet the Smart Home experience on the other hand. With IoT, scale should not be an issue as the number of transactions will increase exponentially as smart devices continuously initiate micro (data) transactions on behalf of the customer. Managing this growth in a compliant and secure way, however, is a different matter as existing payment and transaction infrastructures are not ready to process these transactional volumes (see calculation). Additionally, current pricing models are mostly transaction based, which in this context challenges PSPs to rethink their pricing strategy. New solutions that match the needs of customers and merchants whilst taking note of the current infrastructure capabilities offer new opportunities.

Collaboration key for success

Smart Home offers the opportunity to fully unburden the customer and increase relevancy. Tech-giants are already positioning themselves by experimenting with Smart Home platforms and devices and offering payment services to get even more close to customers and become part of their daily lives.

Regardless of how Smart Home will evolve, the wide variety of challenges that need to be addressed by retailers, producers and PSPs are thus complex that solving them in isolation is risky and costly. And with tech-giants moving up the value chain, there is little chance of success. It is therefore imperative to offer personalized end-2-end Smart Home propositions through cooperation in order to create visibility, the necessary scale and become and stay relevant to customers and business partners. The quality of the collaboration between the customer, merchant, producer, PSP and other relevant parties, will ultimately determine success in the long run. And here lies the opportunity for retailers. They are still in pole position to take the lead, organize collaboration within the value chain and amongst retailers, and face the platform competition, but the time to act is now!

Interested? Please feel free to contact us.

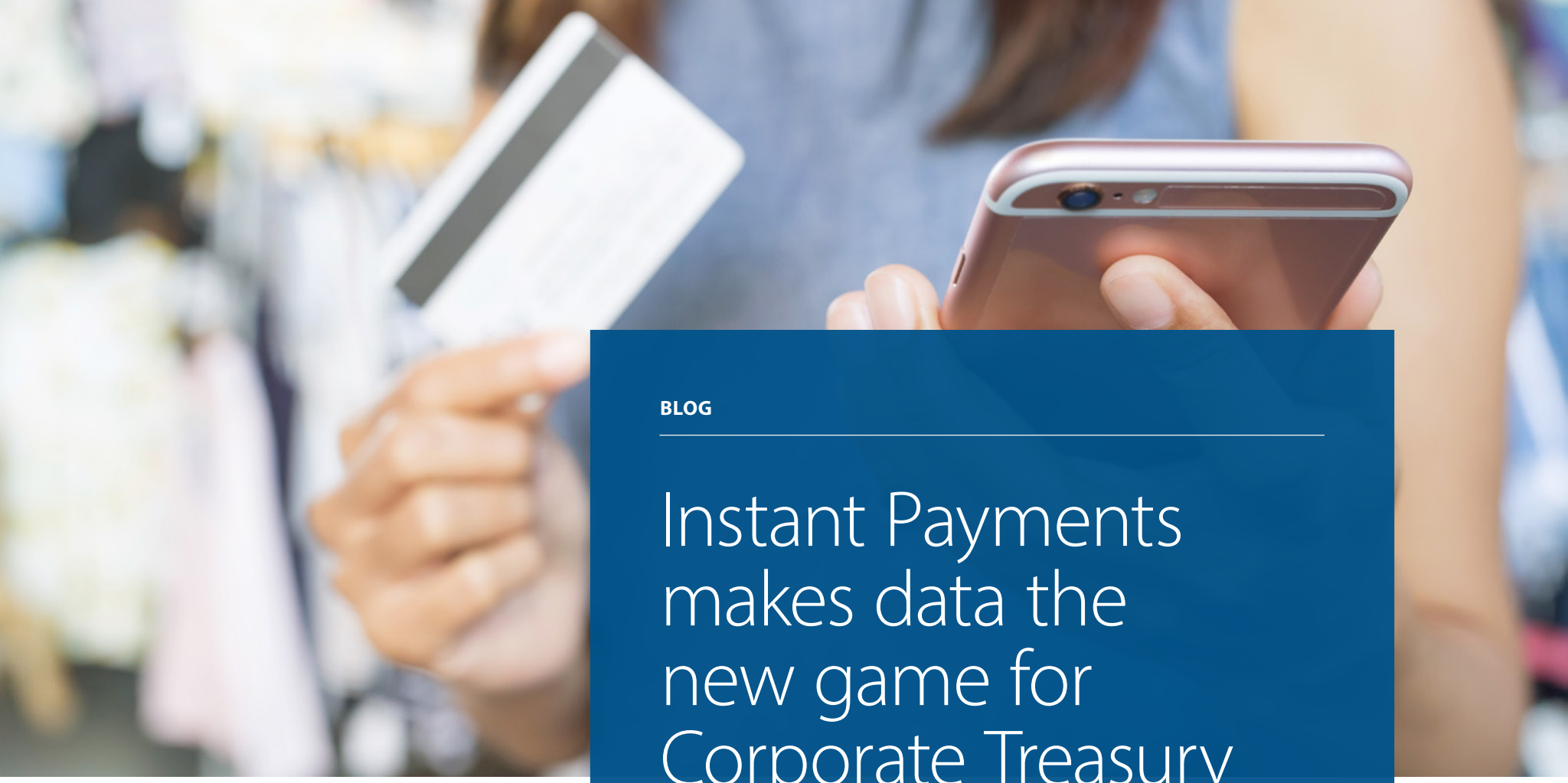
1. https://www.rtlnieuws.nl/editienl/artikel/4258851/niet-thuis-bezorger-z…

Authors

Esther Groen, Denise Hoppenbrouwer and Jim de Wolf

ORIGINAL BLOG

GET IN TOUCH



BLOG

Instant Payments makes data the new game for Corporate Treasury

13 May 2019

Esther Groen

Wouter van den Hengel

Patrick de Haan

GET IN TOUCH

The role of the corporate treasurer will change significantly with the transition towards an open, digital and data driven economy. Partially motivated by regulatory push (eg PSD2, GDPR), organisations are increasingly adopting new business models in which data is shared 24/7 to better respond to instant customer demand. This requires treasury to become data centric.

Data transactions entail (digital) data interactions between departments within an organisation, but also within supply chains and cross sector. In this context, the value of data transactions increases considerably as business processes become more transparent. It enables corporate treasury to better predict cash flows, mitigate transactional risks and forecast liquidity needs. Supported by the roll out of Instant Payment (IP) infrastructures across Europe and other regions, they can now also act immediately.

With the availability of data increasing rapidly and the capability to respond instantly, it makes sense for treasury to pursue a data centric approach. This is a prerequisite for any organisation that wants to successfully operate and participate in an open data economy and society.

Instant payments increase the need for transparency in transactional flows

The IP infrastructure heralds the end of fixed cut-off times as payments are sent and received real-time at any time of the day, any day of the year. The absence of cut-off times challenges treasurers to manage the company's cash position, as payment flows are processed outside current working hours. Treasurers may need to increase reserves to provide for unexpected mismatches in transactional flows. A measure any treasurer would like to avoid.

Insights in data interactions that ultimately result in a payment (ref. figure 1), is essential to accurately predict and control payment flows in an instant around-the-clock environment. Sharing relevant data within and across organisations, creates transparency in business processes and provides treasury with the necessary insights to improve working capital. Enhanced predictability in combination with IP enables the treasurer for instance to reduce mismatches in settling outgoing with incoming funds. As a result, cost related to cash pools and intra-day and overnight facilities can be optimised.

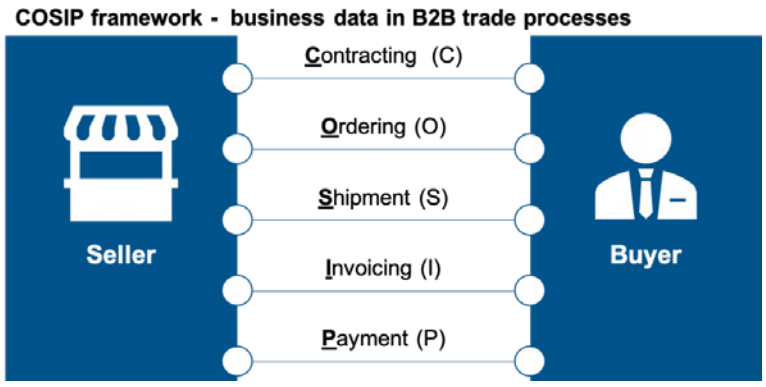


Figure 1. COSIP - framework (see earlier publication [1])

Data sharing enables transparency in transactional flows

The availability of data has increased significantly due to the digitisation of business processes. However, accessibility to data is still lagging. A lot of data still resides in silo-ed and or closed systems (eg TMS, ERP or banking applications), making it difficult for treasurers and other stakeholders (e.g. invoicing, procurement, logistics) to share and apply data effectively.
A data centric approach to treasury is therefore pivotal to optimally benefit from instantly available (payment) data. However, this is easier said than done. Similar to payments, data sharing also comes with high responsibilities. It needs to be secure, comply with regulation (eg consent based), and safeguard the value for all parties involved. To successfully share data, organisations need to develop the following three capabilities: data Availability, data Accessibility and data Applicability. The picture below illustrates how data sharing could work for corporate treasury when implementing and mastering this 'triple-A framework'. For detailed description of the Triple-A framework, please have a look at the EBA report supported by INNOPAY: Data Exploration Opportunities In Corporate Banking.

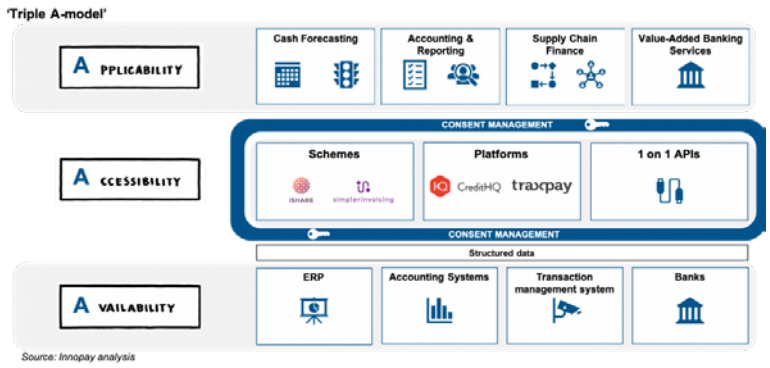


Figure 2: Example Triple-A-Model for treasury

In short, the data availability layer represents the source where data is generated and or stored. The accessibility layer is the way data is disclosed from the source to an application. This can be achieved using 1-on-1 APIs, a platform or a collaborative scheme defining a common set of agreements across organisations. In the applicability layer, data is converted to information delivering the insights treasury is seeking to create value in managing intraday liquidity, cash forecasting and FX risks, for instance.

However, relevant payment data originates in multiple business processes and resides mostly unstructured in even more systems. Systems that do not yet provide for a transparent recording of data to accommodate relevant insights.
When sharing data intercompany or across organisations, managing access and consent crucial. As with payments, treasurers should be in control and thus able to determine specifically what data is shared with whom, at what time and for what purpose.

Finally, by using automated business logic and AI, treasury can further enhance their capability to act 24/7 to instant changes in transactional flows. Already, we see Fintech companies (Highradius and Asterian, for instance) stepping into this space by offering services that deliver data-based treasury insights.

Future corporate treasury is data centric

As the world is increasingly being disrupted by open business models and around the clock availability of products and services, the roll out of IP infrastructure can be considered as a simple hygiene factor. It is only a matter of time until the corporate treasurer will experience a similar disruption. Data is the new game and a data-centric treasury is pivotal to successfully navigate organisations into open, secure, and profitable data driven business models.

1. Digital consent management is key for data opportunities

Authors

Esther Groen, Wouter van den Hengel, Patrick de Haan

ORIGINAL BLOG

GET IN TOUCH

BLOG

Facebook's Libra: the ultimate trust infrastructure or just another institution?

24 June 2019

Shikko Nijland

Douwe Lyclama

GET IN TOUCH

Facebook's new cryptocurrency Libra is not merely about transactions; it's also about trust to a certain extent, but mainly it's about world dominance. In this blog, we explain why.

Last week Facebook announced the launch of Libra, a new global cryptocurrency and financial infrastructure built on blockchain technology. It also announced a new digital wallet for Libra, called 'Calibra', that will be available in the whole of the Facebook universe. In conjunction with 28 partner companies, Facebook claims it is creating a more "inclusive" financial ecosystem. The Libra mission is to create a financial infrastructure "that empowers billions of people…so people everywhere can live better lives". In our book Everything Transaction,we describe two major root causes that need to be addressed to fully benefit from the digital transformation and to realize a truly transactional, financially inclusive economy: trust, and data benefit balance. Libra claims to be aimed at addressing precisely those two issues. But if we take a closer look, it becomes apparent that this cryptocurrency is not really about payments after all.

Libra's claims

1. Helping the unbanked
2. Reducing remittance costs for migrant workers
3. Easy p2p payments for Facebookers.

1. Helping the unbanked

Libra sets out to help the unbanked, amounting to 1.7 billion people including <1% of people in the Netherlands and 7% of US citizens. In terms of how Libra could fundamentally help them, let's not forget that there is a reason why people are unbanked. According to the World Bank (2014), the main reasons are: 1) They don't have enough money, and 2) They don't need a bank account. So how will they get money in and out of their Libra wallet?

On a positive note, a World Bank report indicates that 100 million unbanked people could become financially included if government wages, pensions and social benefits could be paid directly into an account. The same report states that digital payments offer other opportunities to increase account ownership and use; more than 200 million unbanked adults who work in the private sector are currently paid in cash only, as are more than 200 million who receive agricultural payments.

A 'minor' detail: in order for these unbanked people to be included, the underlying assumption is that they will all need to have Libra wallets such as Calibra.

2. Reducing remittance costs for migrant workers

Libra has published a white paper which states that the average remittance cost for tranferring US$200 is 7.01%. Besides the significant differences per corridor, the whole remittance ecosystem committed itself to reducing the average cost to <3% by 2030. In other words, this problem is already being addressed and is likely to be solved, with or without Libra.

It should also be kept in mind that cash is still king in almost any retail business in most developing countries. The underlying challenge is not about the lack of access to a global transaction infrastructure. The biggest and most expensive aspect for all tech/mobile solutions – including Libra – is cash conversion, or the ability to use it as currency within the closed-loop system. Even 'poster child' mobile phone-based money transfer, financing and microfinancing service M-Pesa still has over 40,000 local agents to distribute and convert cash. The main raison d'etre for withdrawal networks has less to do with people not having a bank account, and more to do with the dominance of cash on the streets.

Therefore, the bigger problem to solve in order to break this vicious circle is how to ensure enough migrant workers have a wallet. If they don't have a bank account now, how likely is it that they will pass the 'know your customer' (KYC) procedure for Calibra or any other cryptowallet? If the Libra consortium fails to solve this issue, it may even have a negative impact on financial inclusion because besides the unbanked there will also be a new group of 'non-walleted' people.

3. Easy p2p payments for Facebookers

But in the considerations above, we're almost forgetting the 'Facebook citizens'. This is where it gets really interesting, because you could arguably consider Libra the representation of what we have described in our book as 'infrastructural trust as the replacement for institutional trust'. The Libra infrastructure is a blockchain-based and therefore undisputable single source of truth that can be used for transactions, but also for exchanging (personal) data and storing your digital identity. Users should be aware that the Libra infrastructure, by design, records all transactions and makes them visible to the entire network – and what a network that is, with around 2 billion active users on Facebook, Messenger and WhatsApp! And last but not least: Libra is an institution, a company which invests the Libra proceeds into liquid assets… fiat and government bonds of selected governments. So another middleman, albeit in a category of its own, with the profits going to the middleman's shareholders.

Facebook does not yet seem to enforce a direct link between Calibra and a Facebook account. However, it is highly likely that if you want to use Libra for micro transactions within the Facebook universe or want to monetize your personal data, you will have to give your consent to link your Calibra (or any other wallet) to your Facebook, WhatsApp and Messenger account. Only then will you be able to fully benefit from the trust infrastructure that facilitates seamlessly integrated payments and data transactions.

By design, Libra could make peer-to-peer (p2p) payments easy, seamless and safe – but is it worth paying the privacy price? Facebook already knows everything about your non-financial life; now, it gains insight into your financial life as well. There will be believers and non-believers, but one thing is for sure: with this latest development, Mark Zuckerberg is giving the term 'financial inclusion' a whole new meaning…
As with many platform solutions in a two-sided market, there is huge potential but that will only be realized after mass adoption. Considering the client base and the consortium partners, they may succeed. But for now it remains to be seen how much – if any – value this innovation adds and how the data benefit balance will look. Without mass adoption, this is not a 'killer' finance use case and it is unlikely to succeed, neither in the rich countries nor the poor countries nor within the Facebook universe.

So if Libra is not really about payments, what is it about? Libra is poised to become the world's largest institution by creating a trust infrastructure connecting people right around the globe, introducing a 'full reserve tokenized semi-fiat currency' and taking ownership of digital safety and security.
Libra (through Facebook and its impressive consortium) is the first and maybe only organisation to have such immense cross-border power and thus such a big responsibility to combine and leverage both institutional and infrastructural trust at a global scale. Beware: Libra may appear to be a consumer product, but its hidden power may lie in the potential to disrupt existing banking, trade-lane and FX services, and could even be regarded as a potential replacement of the internet. There is clearly much more to it than meets the eye, so INNOPAY will continue to monitor the developments.
For the latest insights into how digital trust and data sharing will impact your ecosystem, don't hesitate to contact us.

Authors
Shikko Nijland and Douwe Lycklama

ORIGINAL BLOG

GET IN TOUCH

BLOG

INNOPAY helps organisations to improve their agility and decisiveness with hybrid teams

26 June 2019

Matthijs Ros

In today's digital transformation, organisations must be fast, agile and decisive in order to continue to meet the ever-changing needs of customers in the digital era. At INNOPAY, we guide organisations through this digital revolution. By sharing know-how from our consultancy services and then executing the resulting insights – by forming teams made up of internal talent supported by external experts – we can make a tangible difference.

Agility means that an organisation can change direction quickly and effectively whenever that is necessitated by the market conditions. That ability – supplemented by the necessary decisiveness – is crucial in order to stay relevant in the eyes of the customer... and that can be pretty challenging. Research has shown that around 70% of all digital transformation initiatives fail, often due to poor collaboration or a lack of talent [1].

Organisations spend a disproportionate amount of time and money on finding and nurturing the best individuals, especially in the digital domain where the 'war on talent'is raging particularly fiercely. Besides that, the specialization trend is making it even more difficult to define the right search criteria... because how can you look for the right person if you don't know who you want to find? The flexibilization of the labour market is creating an extra problem: how can you ensure successful collaboration between talented professionals who don't want to join your workforce and those from within your own organisation?

GET IN TOUCH

INNOPAY

The strength of hybrid teams

INNOPAY has access to a pool of more than 200 talented professionals in the field of digital transformation. Whenever specific know-how is required, whether in response to a customer request or not, we select the best specialists from the pool and arrange for them to work closely with our own in-house experts. This results in the optimal hybrid team for each assignment. All the team members move to the beat of the same drum and share a single goal: to achieve the best end result for the customer.

Quality is a top priority for us, which means that our aim is to always have the right person on the right spot. We are able to deliver on that promise thanks to more than 15 years of experience in the area of digital transactions. We not only know the market like the back of our hand, but we also have a large, close-knit network of the very best experts on all aspects of digital transactions: legal, marketing, cybersecurity, identity management, project management and programme management. This network is what gives us the edge.

Our people are our assets – irrespective of whether they are on our payroll or not. We keep them close to us, such as through our own Academy: a quality programme that provides training, education and inspiration sessions to everyone, whether they are our in-house specialists or specialized freelancers.

We firmly believe that our hybrid teams enable us to offer our customers even greater peace of mind. We choose talented freelancers who are the perfect addition to our own in-house talent – and in many cases we have been working with them for years, which maximizes each project's likelihood of success. In other words, our network not only enables us to be flexible in our response to the needs of our customers, but also to optimally guide them through the digital transformation.

1. IDC

Author
Matthijs Ros

ORIGINAL BLOG

GET IN TOUCH

BLOG

Het doordelen van hypotheekdata straks net zo makkelijk als ‘appen’

5 July 2019

Esther Groen

Tien jaar geleden had niemand van ‘appen’ gehoord, en nu is het niet meer weg te denken uit ons dagelijkse leven. Wij hebben in korte tijd collectief ons gedrag aangepast en ‘appen’ als werkwoord aan onze vocabulaire toegevoegd. En er komt alweer een nieuw woord aan: doordelen. Het doordelen van je eigen gegevens, zodat je niet meer overal alles opnieuw hoeft in te vullen. Hierdoor wordt jouw informatie op minder plekken vastgelegd. Technologie maakt het mogelijk en wetgeving vereist dat consumenten in 2019 volledige controle hebben over persoonlijke data, ongeacht waar deze is opgeslagen. De hypotheeksector kan hierin een sleutelrol vervullen door te faciliteren dat consumenten zelf bepalen wie toegang krijgt tot persoonlijke (financiële) data, wie er gebruik van mag maken en wie iets mag toevoegen of doordelen in de keten. Doordelen wordt een nieuw soort transactiedienst, deze keer niet met geld, maar met data.

Klanten willen meer controle over persoonlijke data

Nog meer dan bij de televisie, waarbij de afstandsbediening de kijker zicht geeft op de hele wereld, heeft internet de consument toegang gegeven tot de wereld. De smartphone is de ultieme mobiele afstandsbediening die controle (terug)geeft aan mensen. Niet meer alleen vanuit huis, maar vanaf iedere plek, op ieder moment, wanneer de consument het wil. In de financiële sector zien we dezelfde ontwikkeling. De sector bevindt zich in een overgangsfase van ‘customer centric’ naar wat we bij INNOPAY ‘control centric’ noemen. Hierbij bepaalt de klant zelf wie er toegang heeft tot

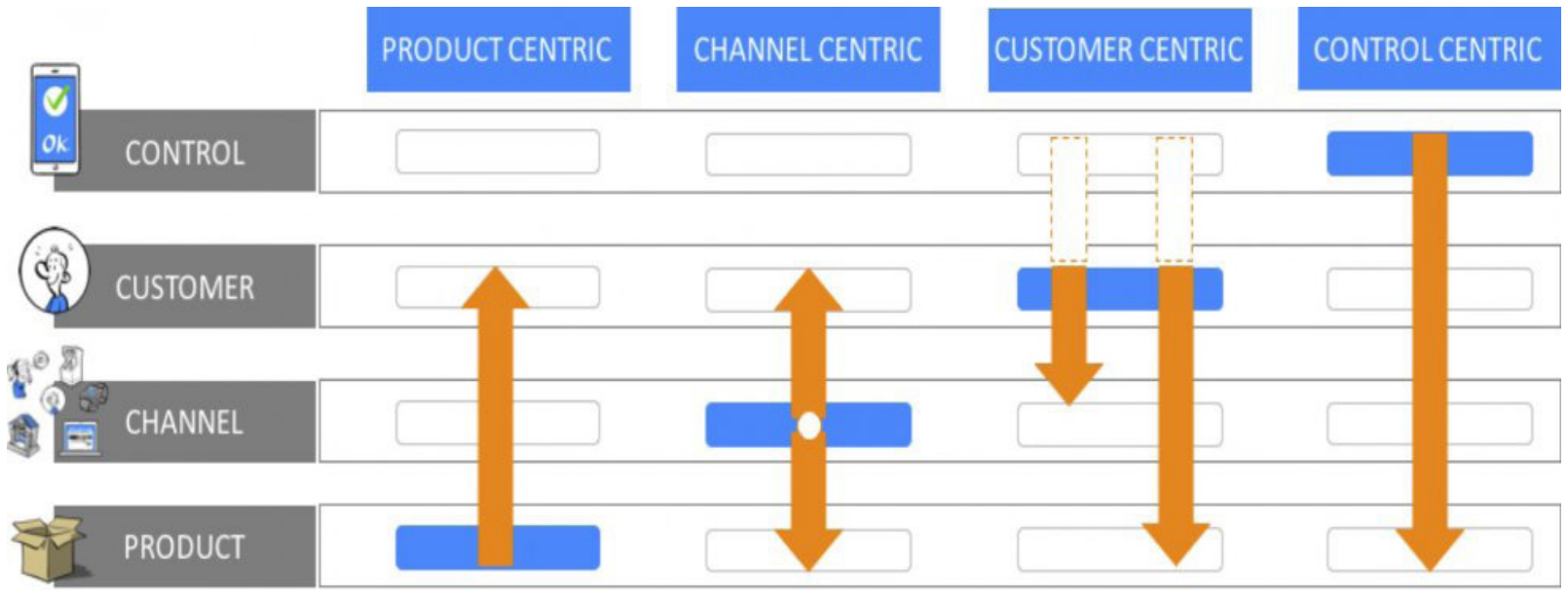
GET IN TOUCH

INNOPAY

zijn data en wat deze partij ermee mag doen. Ook de keuze voor het kanaal en product ligt bij de klant. Deze transitie is weergegeven in figuur 1. Bij banken en fintechs is dit zichtbaar in de ontwikkeling van het 'open banking' concept, maar ook binnen de hypotheeksector ontstaan steeds meer vergelijkbare modellen.

Om volledig 'control centric' te worden met betrekking tot data, moeten hypotheekbedrijven en -ketens in ieder geval een doordeelstrategie ontwikkelen. Daarin moet vastgelegd worden hoe bedrijven hun klanten faciliteren om eenvoudig en veilig data van anderen te hergebruiken, welke data extra moet worden vastgelegd en hoe opgeslagen data wordt doorgedeeld. Uiteraard allemaal op een veilige en compliant wijze, zoals we gewend zijn bij financiële transactiediensten.

De Europese wetgeving geeft twee 'control centric' richtlijnen die grote gevolgen hebben voor de manier waarop met persoonlijke betaalrekeningdata moet worden omgegaan: Payment Service Directive 2 (PSD2) en General Data Protection Regulation (GDPR). Deze laatste gaat verder dan financiële gegevens. GDPR geeft nog meer controle aan klanten over persoonlijke data door organisaties verplichtingen op te leggen ten aanzien van inzage, veiligheid, portabiliteit en het recht om vergeten te worden.



Digitaal vertrouwen creëren door klant controle te geven

Het huidige internet is helaas nooit gebouwd om transacties te ondersteunen. De wijze waarop vertrouwen erin is verankerd is verre van optimaal. Het is daarom nog geen volwaardig transactiekanaal en zeker niet voor gevoelige hypotheekproducten en diensten. Bij het creëren van een digitale vertrouwensrelatie met klanten moet de zogenaamde vertrouwensparadox worden doorbroken. Hiermee bedoelen we de tegengestelde behoefte van gebruikers om data, en dan met name persoonsgegevens, meer toegankelijk te maken én veel beter te beveiligen, om zo hun digitale vertrouwen in de ander te versterken. Digitaal vertrouwen kan worden gerealiseerd door de consument controle over 'zijn' hypotheekdata te geven. Dit zou kunnen door de klant in staat te stellen om zijn financiële data die zijn bank al van hem heeft, gemandateerd door te delen. Of liever nog toegang tot zijn data gecontroleerd beschikbaar te stellen aan de rest van de keten.

De informatievraag aan de klant wordt dan anders: "Mag ik uw data krijgen?" wordt vervangen door: "Wilt u mij tijdelijk toegang tot uw data geven?". Welke van deze twee vragen zou de vertrouwensrelatie met uw klant het meest versterken?

Datadeel-afsprakenstelsel in hypotheeksector

Bij INNOPAY geloven we in de kracht van samenwerking, juist in de digitale wereld. Dit zien we niet alleen bij het openbaar vervoer, waar we samen met tien vervoerders en Translink werken aan de opvolger van de ov-chipkaart. Maar ook in de logistieke sector waarin we samen met grote logistieke partijen een vertrouwensinfrastructuur iSHARE ontwikkelen om datadelen tussen ondernemingen te vergemakkelijken. In de financiële sector zien we succesvolle samenwerking tussen banken bij pinnen, iDEAL en iDIN.

Onderlinge samenwerking in de hypotheeksector met nieuwe innovatieve fintechs is helaas nog te zeldzaam. De structurele samenwerkingen die er wel zijn, lijken vooralsnog meer op een gedwongen huwelijk, terwijl er toch duidelijk wederzijdse voordelen zijn. Het steeds breder inzetten van Application Programming Interfaces (API's) zorgt ervoor dat het doordelen van data meer gecontroleerd en gebruikersvriendelijk kan

gebeuren. Daarnaast zorgt het ervoor dat er compleet nieuwe (open) business en service modellen kunnen ontstaan, omdat hypotheekproduct- en distributiestrategieën schaalbaar kunnen worden gemaakt.

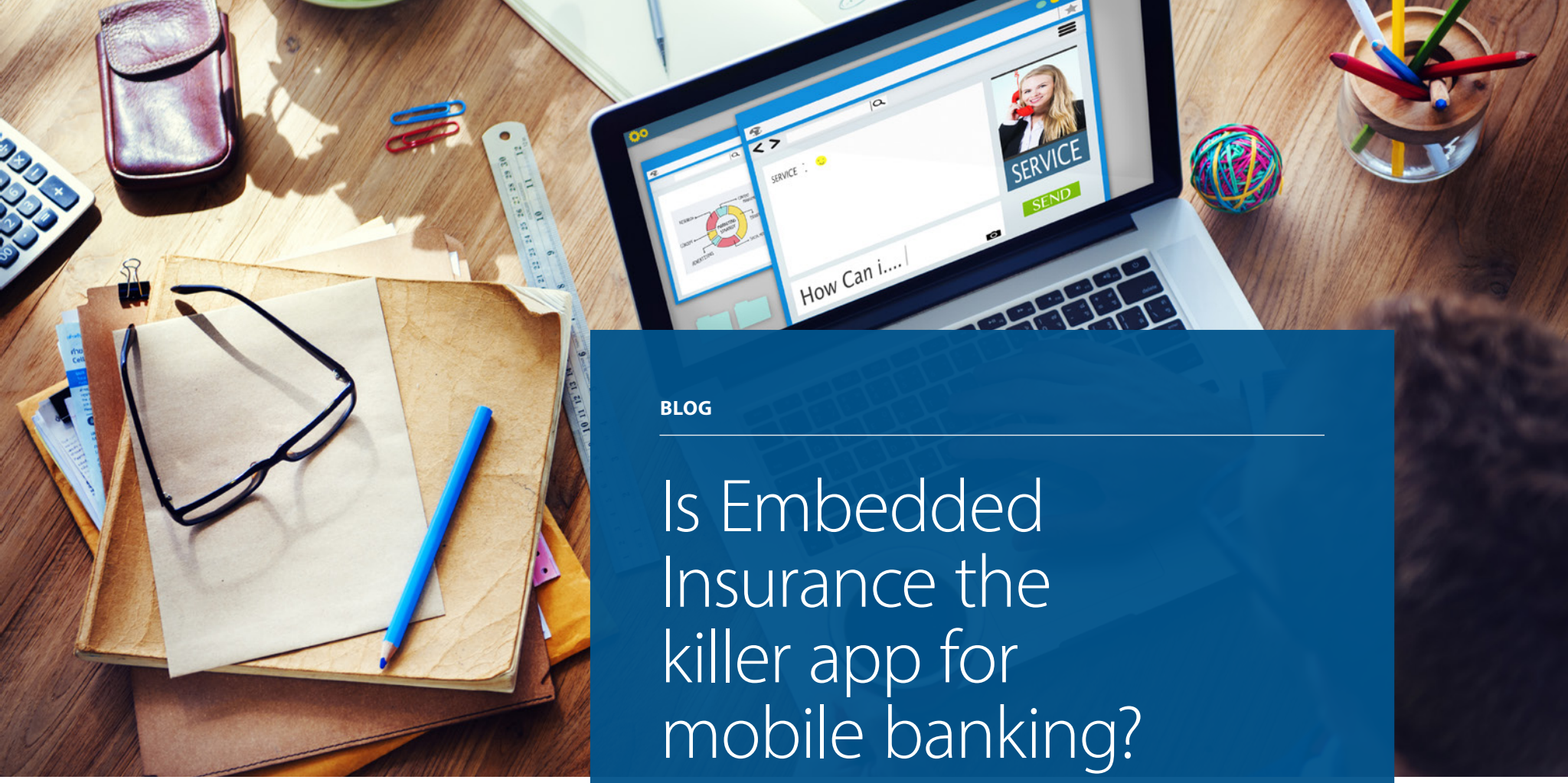
In 2017 heeft INNOPAY de voordelen van samenwerking in de hypotheekketen onderzocht in opdracht van HDN. Met een brede ketenvertegenwoordiging zijn verschillende samenwerkingsinitiatieven voorgesteld met als doel de risico's op GDPR non-compliance te minimaliseren voor alle partijen in de keten. Deze initiatieven dragen echter ook in belangrijke mate bij aan het verbeteren van de klantervaring doordat er afspraken worden gemaakt over hoe bijvoorbeeld de regie van de klant in de gehele keten transparant te maken en toe te passen.

Als we het hebben over zo'n samenwerking, kan bijvoorbeeld worden gedacht aan het gemeenschappelijk ontwikkelen van een datadeel-afsprakenstelsel. Dit zou de ontwikkelkosten relatief laag houden en de kans op sectorbrede adoptie vergroten. Het resultaat is dat het voor klanten makkelijker en laagdrempeliger wordt om alle relevante hypotheekdata snel, juist en volledig beschikbaar te stellen voor de hele hypotheekketen. Bovendien kan een dergelijk afsprakenstelsel ook als basis dienen voor nieuwe open businessmodellen met partijen binnen en buiten de sector. Hierdoor wordt het doordelen van hypotheekdata voor klanten net zo makkelijk als appen. En dan is ook 'doordelen' straks niet meer weg te denken uit ons dagelijks leven.

Author
Esther Groen

ORIGINAL BLOG

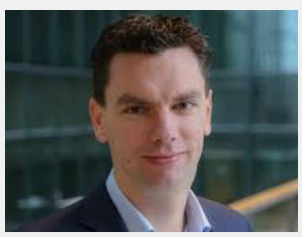
GET IN TOUCH



BLOG

Is Embedded Insurance the killer app for mobile banking?

19 July 2019



Maarten Bakker

GET IN TOUCH

INNOPAY

As the number of digital transactions is growing exponentially, companies who have relevant and frequent digital interactions with their customers compete to become future ecosystem orchestrators. This is also true for the banking sector, where customers are increasingly banking through their smartphone, making that the primary digital source of point of sale and point of contact for financial products and services.

INNOPAY has analysed the bank's mobile insurance propositions and revealed that Neobanks and incumbent leaders are embracing Embedded Insurance models. In this blog, five key Embedded Insurance trends are presented which will shape the next generation of the traditional €360 bn. GWP European bancassurance model. Incumbents should take notice and act.

WHILE MOST INCUMBENTS REMAIN LOCKED IN TRADITIONAL MODELS, INCUMBENT LEADERS AND NEOBANKS ARE REDESIGNING THE €360 BN. GWP EUROPEAN BANCASSURANCE MODEL FROM THE GROUND UP

Figure 1: User flow of selected Embedded Insurance propositions

In traditional bancassurance distribution models, banks have dedicated partnerships and are the point of sale or point of contact for the sale of insurance products. Banks earn additional revenue by selling insurance products, while insurance companies can expand their customer base without having to expand their sales force. The mutual beneficial and integrated relationship has led to high market shares for banks in the distribution of insurance products (~30% of total Gross Written Premium (GWP) in 2016 in Europe [1]).

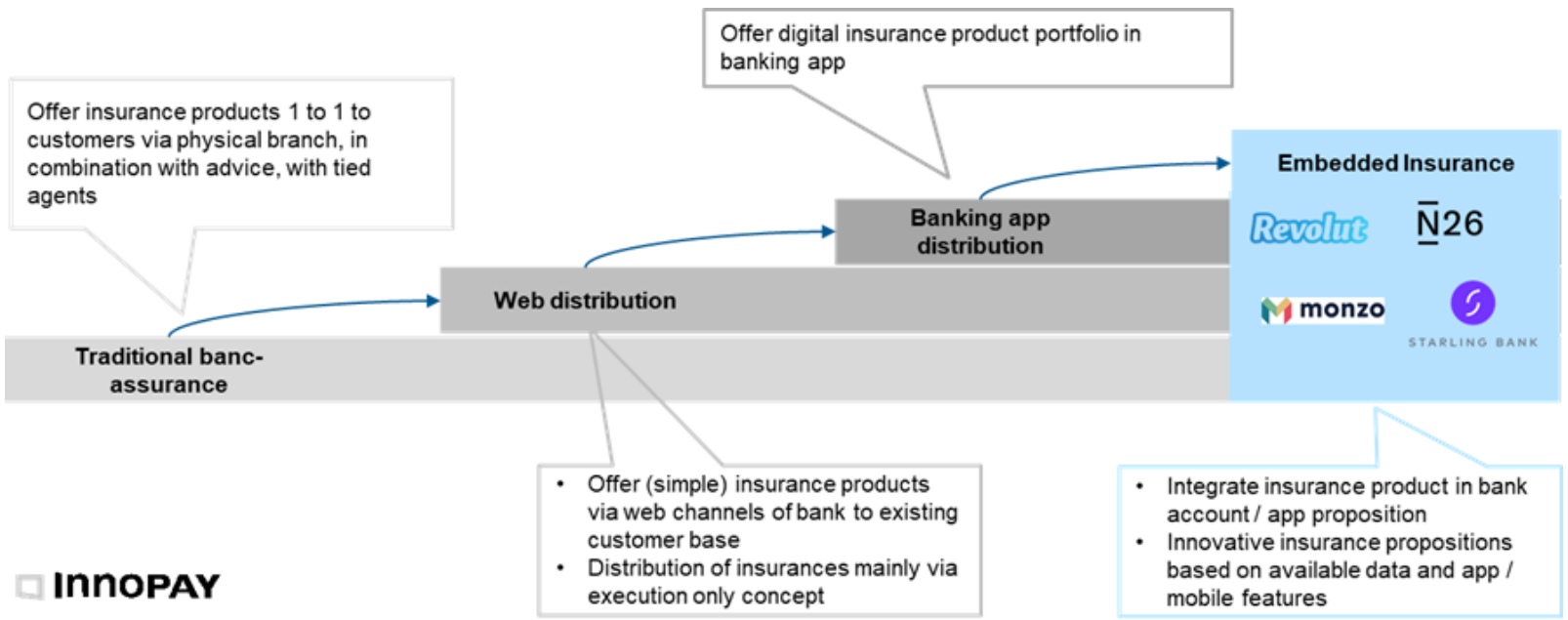


Figure 2: Evolution of bancassurance; Source: INNOPAY analysis

This model has suited the financial industry for many decades and is now slowly moving towards banking apps. INNOPAY has analysed these mobile insurance offerings and models across the banking sector, showing that Neobanks and incumbent leaders are embracing Embedded Insurance models. In this they are unique in combining the different distribution and advice models in a mobile only platform proposition.
The payment account in combination with a fully conducted bank-grade KYC process, is used as an anchor to daily engage with the customer and provide them with innovative insurance propositions.

For example, Revolut gives an entire digital experience where the user can onboard for the insurance and likewise report a claim in their banking app within minutes. Secondly, travel insurance is offered, which fits in to the Neobank's target group needs – Millennial Travelers. Some Neobanks provide their customer base with a flexible and usage-based insurance policy for their travels. An example is Revolut's Pay-per-Day overseas medical insurance which uses geolocation technology, so the insured person only gets charged for the days that they are abroad. And N26 has partnered with German InsurTech Clark to enable customer to capture and manage all insurance policies in one place. The customer has a more transparent overview and can switch easily to more beneficial insurance policies.

Five trends to guide incumbents when reshaping their next generation bancassurance strategy

Locked-in to decades old dedicated partnerships, legacy products, legacy propositions and legacy systems most incumbents have only just started moving their current propositions to their mobile banking environment. In taking this approach they are losing out on the innovation opportunities the mobile banking platforms can bring to them. Leaders and Neobanks are grabbing these opportunities and the customer growth, which these banks are experiencing, is significant and continuous. For example, N26 has recently announced that its customer base grew from 1 million (June 2018) to 3.5 million (June 2019) within a year [2].

INNOPAY identified five key trends for Embedded Insurance in banking which incumbents should act upon to stay relevant.

1. Selective partnerships

Selecting dedicated partnerships for a specific product, geography and/or customer segment can make sure that the products and services offered are a perfect fit with the overall promise of the bank. If executed correctly this will lead to a perfect customer experience, leading to high in-app conversions with low price sensitivity. ING and AXA have announced a partnership in 2018 for specifically this purpose [3]. But also Neobanks are carefully selecting their partners to build their insurance propositions.

2. Platformation of insurance

To be able for banks to offer the most innovative insurance products and speed up implementation time new InsurTechs are entering the scene with platform propositions. These parties can facilitate new (API based) integrations of different services in the customer journey. Well known examples of

these new platforms are BSurance, SimpleSurance and the Lemonade API.

3. Insurance and service marketplaces

To be able for banks to offer the most innovative insurance products and speed up implementation time new InsurTechs are entering the scene with platform propositions. These parties can facilitate new (API based) integrations of different services in the customer journey. Well known examples of these new platforms are BSurance, SimpleSurance and the Lemonade API.

4. Use of new data sources

Transaction data is a rich source of information for triggering advice or buying suggestions. But also, the registration of high-value items, risk assessments or fraud detections could be done with transaction data. Mobile banks can easily organize customer consent between data sources and users and, possible enriched with PSD2 aggregated data from other accounts, are well positioned to take advantage for new innovative insurance propositions. Next to that mobile banking apps, with a fully conducted bank-grade KYC process, are a logical place to also consume other data sources with customer consent (connected cars, social, Gmail etc.). These other data sources can even provide more meaningful context and the possibility of shaping insurance innovation at scale.

5. Retail product and insurance integration

Insurance is more and more integrated in the product or service a customer is buying. One of the more quoted examples is Tesla, which is including a car insurance in the total service package of its car. And given that banks can have real-time insight in important aspects of your behaviour they for example can automatically insure your high-value items or link your account to other data sources which can trigger insurance coverage. This enables banks to develop mobile insurance propositions (or provide a platform to solution providers) which fit with the overall promise they make to the customers, a careless and seamless experience.

Based on discussions with senior executives, INNOPAY sees several questions which incumbents need to answer before they act:

- What are the needs of our current and future customers with regards to insurance and how can we serve them?
- How does our bancassurance strategy fit with our mobile strategy & open data / PSD2 initiatives?
- Which mobile platform, open data / banking / PSD2 initiatives are we leveraging to shape new innovative insurance propositions?
- What are we learning from Neobanks, InsurTechs and their insurance propositions?
- How do we develop our mobile app capabilities and operating model for new insurance propositions?

Want to know how much of the €360 bn. GWP European bancassurance can be yours? Please contact Maarten Bakker (maarten.bakker@innopay.com) to discuss the latest insights or to request the full Embedded Insurance radar which contains Embedded Insurance cases and related trends across different digital ecosystems.

Written in collaboration with Joris Eckrich.

1. https://www.insuranceeurope.eu/sites/default/files/assets/DatabaseMarch2019_Distribution.xlsx

2. https://n26.com/en-eu/blog/were-celebrating-3-5-million-customers

3. https://www.ing.com/Newsroom/All-news/Press-releases/ING-and-AXA-announce-digital-partnership-to-build-a-global-insurance-platform.htm

Author

Maarten Bakker

ORIGINAL BLOG

GET IN TOUCH

BLOG

Datasleutelkastjes als wapen tegen dominantie techreuzen

7 August 2019

Shikko Nijland

Het kabinet maakt zich zorgen om de toenemende macht van de grote techreuzen. Het wil de dominantie van deze partijen terugbrengen en bepleit een Europese aanpak. Willen we afhankelijkheid van de grote platforms echt voorkomen, dan zullen we niet alleen moeten nadenken over hun marktpositie, maar ook over hoe we de controle houden over onze eigen data. Een nieuwe 'soft' infrastructuur biedt uitkomst.

In ons boek 'Alles Transactie' leggen we uit dat we op de drempel van een volgende fase van het internet staan. In het transactionele internet is data het nieuwe goud. Het verzamelen van data is een serieuze business geworden waarmee nieuwe diensten en producten worden ontwikkeld. Echter, de keerzijde hiervan is dat er ongewenste en onzichtbare beïnvloeding van grote groepen mensen plaatsvindt en zich diverse privacy issues voordoen. Willen we profiteren van de voordelen van het transactionele internet zonder overgeleverd te worden aan de dictatuur van techreuzen, dan zullen we de controle over onze eigen data beter moeten regelen.

GET IN TOUCH

INNOPAY

‘Soft’ infrastructuur regelt de controle over data

In plaats van dat we massaal data overbrengen naar de grote platforms, houden we data bij de bron. Het is technisch mogelijk om data fysiek bij de eigenaar van de data te houden. Met een set uniforme afspraken en standaarden – een ‘soft’ infrastructuur’ - geven we gebruikers de controle over hun data.

Deze uniforme afspraken en standaarden maken dat data-eigenaren met behulp van hun eigen datadeelsleutelkastje zelf kunnen beslissen aan wie ze hun data verstrekken en onder welke condities. Hij heeft een dashboard binnen de ‘mijn’-omgeving van zijn datadeelsleutelkastje waarin hij digitale sleutels toekent met behulp van bijvoorbeeld aan / uit schuifjes of buttons voor het verlenen van specifieke toestemming. Ook kan hij reageren met ‘ja/nee’ op datadeelverzoek binnen deze omgeving of via email, WhatsApp, SMS en social media.

Een datadeelverzoek kan komen van verschillende partijen. Bijvoorbeeld, het ziekenhuis vraagt om huisartsgegevens. Of een telecombedrijf wil een laatst gebruikt en door de bank geverifieerd adres zien wanneer een gebruiker zich aanmeldt voor een nieuw abonnement. Of een adverteerder wil in ruil voor data over zijn vakantieplannen of schoenenvoorkeur de gebruiker belonen. De gebruiker is volledig in control en kan alles volgen en managen in zijn datasleutelkastje. In plaats van data te versturen kan de gebruiker bepalen wie zich mag ‘abonneren’ op zijn data. De datadeel keten is nu omgedraaid en daarmee is ook de machtsbalans hersteld.

Om te voorkomen dat een gebruiker bij iedere organisatie een apart sleutelkastje krijgt (fragmentatie), zullen datasleutelkastjes interoperabel moeten zijn en met elkaar kunnen communiceren. Een netwerk van datasleutelkastjes zorgt ervoor dat de sleutels van verschillende organisaties binnen één sleutelkastje worden gehouden. Gebruikers kiezen dan zelf bij welke aanbieder ze hun sleutelkastje(s) willen hebben.

Het is van belang dat leiders in de private en publieke sector de handen ineenslaan om gezamenlijk deze ‘soft’ infrastructuur te ontwikkelen. Want alleen als we data bij de bron houden en de data-eigenaar empoweren maken we ons minder afhankelijk van de grote techreuzen, en nemen we onze digitale toekomst meer in eigen hand.

Author
Shikko Nijland

ORIGINAL BLOG

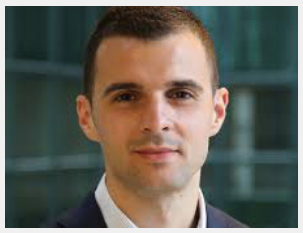
GET IN TOUCH

BLOG

Innopay's TPP RADAR: Europe gearing up to use access to accounts under PSD2

20 August 2019

Luc van Oorschot



Mounaim Cortet

PSD2 is the revised European directive for payment services, with the supporting Regulatory Technical Standards entering into force on 14 September 2019. PSD2 Access to Accounts (XS2A) introduces two new regulated payment services providers: Payment Initiation Services Providers (PISP) and Account Information Services Providers (AISP). Together these are referred to as Third Party Providers (TPPs). The new roles create possibilities for innovation in the European market by enabling market players, with or without a payments background, to create innovative products and services based on the access to a customer's payment account.

All EU Member States have finalised the transposition of PSD2 into national law and are ready to issue TPP licences, and most Member States have already done so. With the TPP Radar, INNOPAY provides insights into the current state of play, by providing an overview of licenced TPPs per country, detailing their background, customer focus, and service offering enabled by their licence.

GET IN TOUCH

INNOPAY

Key findings of INNOPAY's TPP radar

- **mainland EU is catching up with frontrunner UK on the number of issued licences:** the UK alone now makes up for a total of 51% of issued licences, but EU member states are catching up;
- **limited number of licences issued to non-financial services players:** activity from parties with a non-financial services background that obtain a TPP licence is visible, but limited to roughly 10% of the total number of licenced TPPs;
- **market corrects lack of standardisation in PSD2 XS2A through efficient connectivity services:** 28% of B2B focused TPPs offer white label PIS/AIS services, reducing impact, complexity, and costs of connecting to different bank APIs;
- **B2C services enabled by PSD2 evolve in line with market expectations:** 40% of B2C services focus on enabling increased control over personal finances.

Number and type of TPP licence issued per eu member state

The UK is currently the frontrunner in the TPP landscape. Although mainland Europe is catching up, there is still considerable ground to gain. The UK alone has issued a total of 88 licences, versus 83 in mainland Europe. Sweden and Germany follow the UK at a distance, with 16 and 14 licences issued. Figure 1 provides an overview of the number and type of TPP licence per EU member state.

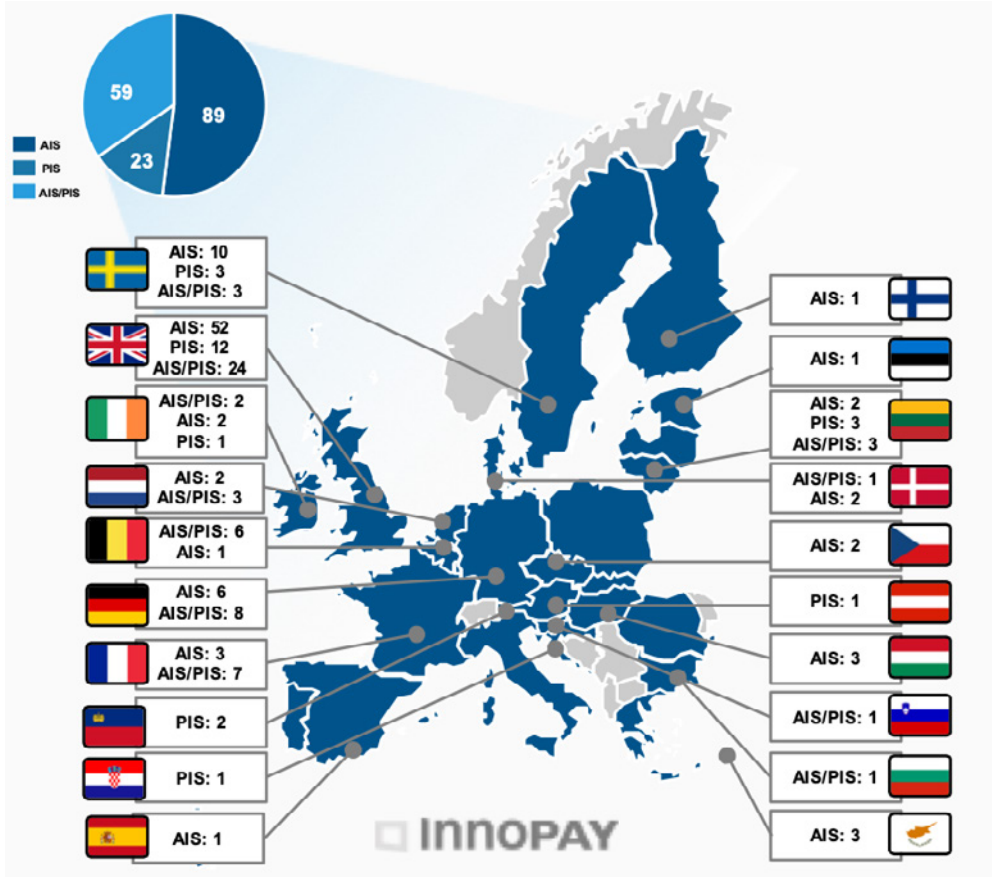


Figure 1: Overview of the number and type of TPP licence per EU member state (analysis as per August 2019)

Background of TPPS

The majority of current licenced TPPs has a background related to financial services. These backgrounds include Personal Finance Management solutions, PSPs, card issuers, credit (rating) providers, and cash management solutions.
Several non-traditional payment players have obtained a TPP licence. Such parties include a telco, loyalty program providers, a grocery store chain, a (retail-) product marketplace, and others. Their numbers, however, are limited to roughly 9% of the total number of TPPs.

There has been market-wide speculation regarding the threat of bigtechs entering the payments market as a result of PSD2 XS2A. Currently, Google is the only bigtech that has obtained a TPP licence (i.e. AIS and PIS licence in Lithuania).

Figure 2 provides an overview of the top-6 categories of TPP backgrounds.

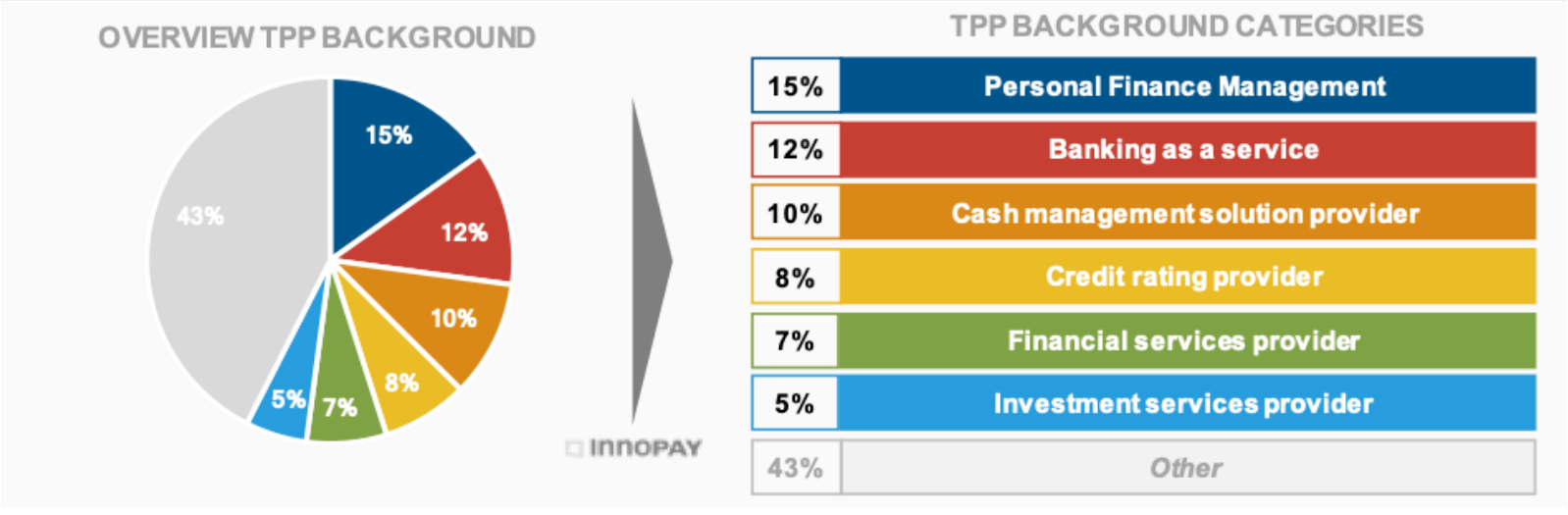


Figure 2: Overview of TPP backgrounds (analysis as per August 2019)

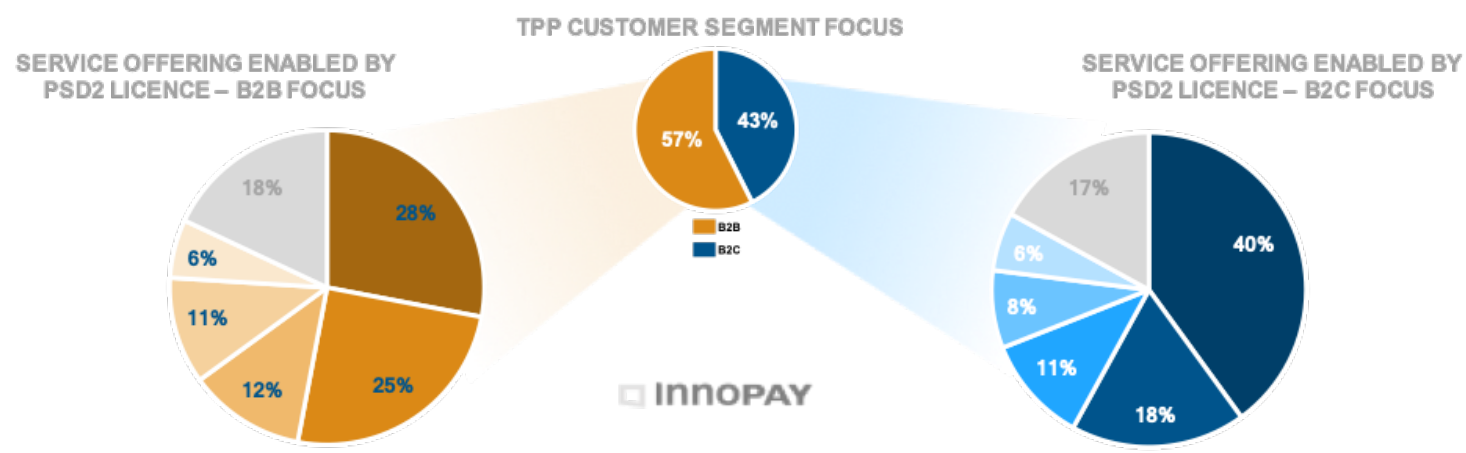
TPP customer segment focus and related service offerings

Only few TPPs have used their PSD2 licence to enable a service offering that lies outside the scope of financial services, yet. With EU-wide issuing of licences in its infancy, and parties outside the financial sector being educated more and more on the opportunities PSD2 XS2A could bring to them, this is expected to change. The customer segment focus of TPPs is currently skewed towards the B2B sector (57% B2B versus 43% B2C).

The largest category of B2B TPP service offerings shows the TPP market addressing the absence of API standardisation, with 28% of TPPs offering bank API connectivity as a service with their white label PIS/AIS services. The offerings of these parties differ, as some focus on mere technical connectivity, while others on value added services such as transaction categorisation, peer benchmarking, or credit scoring.

The largest B2C service offering (Personal Finance Management, 40%) and second largest B2B service offering (cash management solution provider, 25%) lie at the heart of the market's expectations regarding PSD2 use cases, as they revolve around (real-time) insights and actionable applications based on transaction data. Again, here, the service offerings differ in the scope of value added.

The overview of top-5 TPP service offerings enabled by PSD2 licences per customer segment focus is visualised in figure 3.



28%	Whitelabel AIS and/or PIS
25%	Cash management solution provider
12%	B2B payments provider
11%	Credit rating provider
6%	Tax assistance provider
18%	Other

40%	Personal Finance Management
18%	Payment initiation provider
11%	Credit rating provider
8%	Investment services provider
6%	Loyalty program provider
17%	Other

Figure 3: Overview of top-5 TPP service offering enabled by PSD2 licence per customer segment focus (analysis as per August 2019)

Reap the full potential of PSD2 XS2Aa in your sector

More and more, the opportunities of PSD2 are being recognised outside the financial sector.

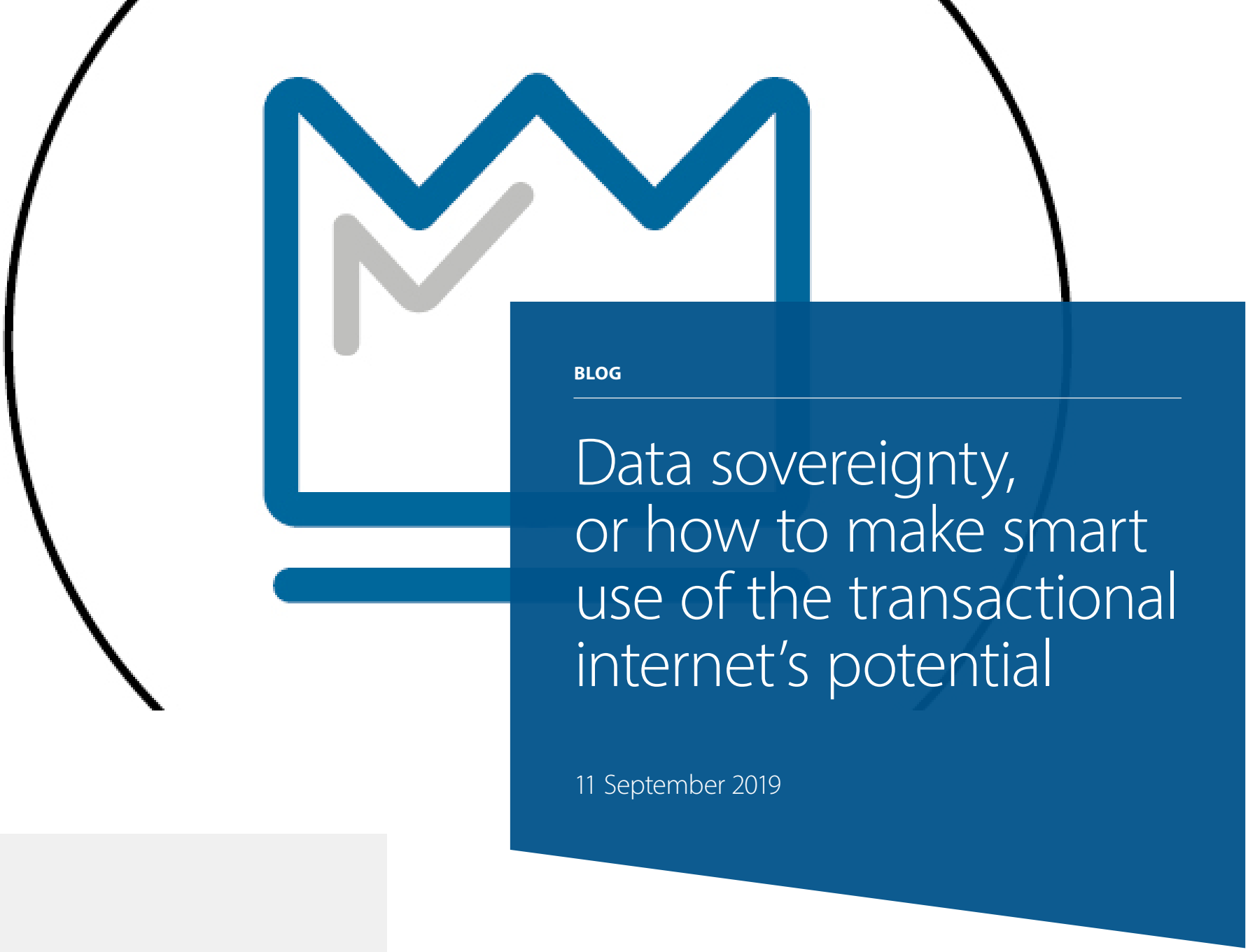
INNOPAY has extensive cross-sectoral experience in enabling organisations to reap the full potential of PSD2 XS2A, with its consulting services ranging from defining your strategic PSD2 XS2A-positioning, to identifying actionable PSD2 XS2A opportunities, and obtaining a TPP licence.
Reach out to us for insights into the full range of TPP backgrounds, TPP service offerings, or if you are interested to find out what opportunities PSD2 XS2A can bring to your organisation.

Authors

Luc van Oorschot and Mounaim Cortet

ORIGINAL BLOG

GET IN TOUCH



BLOG

Data sovereignty, or how to make smart use of the transactional internet's potential

11 September 2019

In an ideal world, data sharing is hassle-free and the transactional internet offers nothing but benefits. The only problem is, that ideal world doesn't exist – at least, not yet. This article takes a closer look at how organisations can make better (i.e. smarter) use of the transactional internet's potential. By providing effective control of data, they can restore people's trust in data sharing – and trust is a fundamental prerequisite for all digital transactions.

The internet was developed in the 1990s as an information medium – initially for researchers, and later for businesses and consumers too. Since then, with millions of people a second now sharing massive amounts of data for a whole range of purposes, it has evolved into the prevailing transaction medium. But the internet is showing signs of strain. It isn't designed to cope with data sharing on such a huge scale, and today's users are never sure whom they can and can't trust.

This has major implications for all digital transactions that involve the exchange of data – and that includes (financial) transactions – because they depend on trust. When purchasing a product or service, for example, the truly crucial moment is when the online customer has to decide whether to click on the 'Buy' button. They will only make that all-important click if they sufficiently trust that the transaction will be completed correctly. Hence, trust is key to the further growth of the transactional internet.

GET IN TOUCH

INNOPAY

Paradox

We are increasingly utilising advanced services that entail more data processing yet, paradoxically, our trust that companies will keep our data secure is diminishing. That lack of trust is understandable because it has been regularly breached in recent years: from consumer details falling into the wrong hands, to the sale of data to third parties and even banks abusing customer payment history for targeted marketing. Consumers increasingly take a critical view of the security and accessibility of (sensitive) information and the sharing of their data – and rightly so.

This lack of trust poses a sizeable challenge for companies because it automatically worsens their relationship with customers, which in turn makes them less willing to share their data. Less data means less relevance, and fewer customers means less revenue. Unless this vicious circle can be broken, it's 'game over' for businesses.

Legislation alone is not enough

With legislation such as the General Data Protection Regulation (GDPR) and the Payment Service Directive 2 (PSD2), governments have taken the first step in the battle against 'data pollution'*. Nowadays we have control over our own data, or at least that's the theory. In practice, however, it appears that legislation alone is not enough. We are presented with countless pop-ups and lengthy statements containing complex terms and conditions and confusing choices, which we often blindly accept.

Data benefit balance out of kilter

Companies are tackling the lack of trust in today's internet – and its technical unsuitability as a transaction network – by building platforms of their own. Platforms profit above all from the revenue generated by data. Despite consumers helping to generate the transactional data, however, they currently receive far from their fair share of the benefits. There is a growing sense that we have little to no control over what happens to our data and how others can use it for profit, which is contributing to the rising dissatisfaction. The 'data benefit balance' is out of kilter, and is currently weighted in favour of just a handful of global tech giants. That balance must be redressed in the consumer's favour, and one way to do so is to put consumers back in control of 'their' data.

Data sovereignty through 'soft' infrastructure

This starts with data sovereignty which gives consumers and businesses control over their data assets without having to store the data centrally. This can be achieved by each data holder implementing a standardised and legally sound identity and consent mechanism.

Such a data sovereignty infrastructure enables data holders to control and monitor who is granted access to their data, to allow their data to be reshared between providers and to give consent to engage in a transactional relationship about the usage of their data. In return they receive a 'data dividend' in the form of a service, credits and/or some other kind of financial value. This will restore the data benefit balance in the transactional internet.

Now, business leaders, policymakers and politicians must come to realise that the societal benefits and economic impact of this 'soft' and invisible infrastructure for digital economic activity is essential to enable the next wave of digital growth and to make smart use of the transactional internet's potential. They need to not only join forces, but also start taking action in their own organisations in order to give people back control over their own data.

The topic of data sovereignty is discussed more comprehensively in the recently published book called Everything Transaction. This book is available for download as of September 23, 2019, via the following link: www.innopay.com/EverythingTransaction

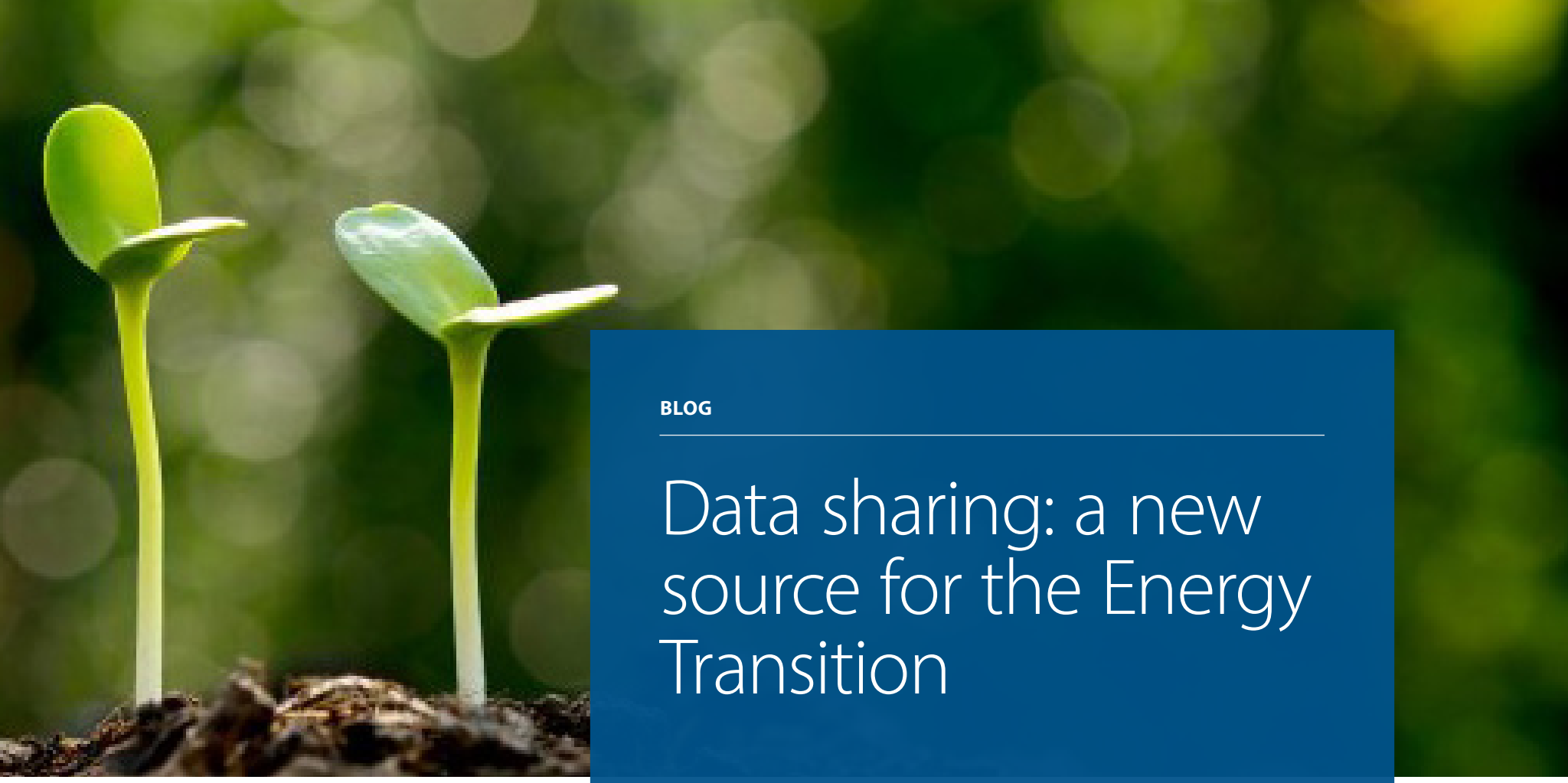
*'Data pollution' refers to the abundance of data in the digital environment and the damage this can cause to citizens and businesses. It arises from the fact that people and organisations have been giving away massive amounts of data for decades.

Author

...

ORIGINAL BLOG

GET IN TOUCH



BLOG

Data sharing: a new source for the Energy Transition

23 September 2019

Douwe Lycklama

Maarten Bakker

Although almost imperceptibly, the number of data transactions is growing exponentially, meaning data stakeholders – consumers, businesses and institutions – have an obvious growing need for more control of their data. At the same time, our energy system has reached a crossroads in terms of its digital future, not least due to the introduction of GDPR, the Climate Agreement and the updating of the Energy Act following the implementation of the Energy Directive as part of the Clean Energy Package.

The topic of 'energy data sharing schemes (or frameworks)' therefore features prominently on the agendas of various stakeholders in the energy sector. Unlike commercial platforms such as Facebook and Google, an energy data sharing scheme gives stakeholders control of data sharing at the source (e.g. registers of grid operators, suppliers or IoT players). This is similar to the way in which data is shared in the fintech sector through schemes such as iDEAL, iDIN and eHerkenning ('eRecognition') in The Netherlands, Maestro across Europe, and iSHARE in the logistics sector. What is more, the concept of an energy data sharing scheme is entirely consistent with the recently formulated Dutch government vision on data sharing.

GET IN TOUCH

INNOPAY

Who can access which data and for what purpose?

The energy sector is already familiar with the phenomenon of data sharing, e.g. in supplier switching and requests for meter data. But these agreements are not futureproof. The growth in the number of data transactions is causing a sharp increase in demand for data sharing, driven partly by the need to shape the Energy Transition. New market players are emerging who need access to data for various purposes, and new data sources are appearing all the time – both within and outside the sector. New assets are constantly impacting the energy system (such as batteries, electric cars, charging stations, solar panels, thermostats and private energy management systems). Active management of these data transactions is urgently needed, not only to maintain system stability but also to sustain the EU energy market's competitive position and to support efficient grid planning and operations.

In short, data sharing is becoming crucial for both regulated and unregulated tasks. The traditional 'in front of and behind the meter' debate is turning into a more generic discussion about access to data: who can access what data under what conditions. These are precisely the complex issues that an energy data sharing scheme can solve.

One single energy data sharing scheme or framework for the whole sector

An 'all-parties' energy data sharing scheme provides a framework within which DSOs, TSOs, suppliers, producers and other parties involved all agree with each other who will have access to which data and how standardized exchanges of data will take place on a level playing field.

Additionally, they agree on ways to maintain the consumer's central position, futureproof consumer control of data and customer journeys. They also take joint cybersecurity measures. These agreements can be made technology-agnostic with no – or very little – new IT (legacy) being used in the core system.

The above-mentioned parties then implement the agreements on a decentralized basis in their own IT systems, processes and organisation. They comply legally with the agreements by means of a (multilateral) contract with a management organisation.

A new basis

The establishment of such an energy data sharing scheme requires a new mindset towards data exchange in the energy sector. Whereas the data sharing governance is currently based primarily on legally described roles and activities, a rigid legislative framework is no longer an appropriate basis for a fast-developing digital world. In the digital domain in particular, new roles are being devised all the time. These roles cannot – and should not have to – be specified in the law in advance. Futureproof governance and its proper implementation must therefore be guaranteed by a non-commercial management organisation.

One of the success factors is a clear distinction between 'how' and 'what'. The energy data sharing scheme focuses on the 'how'. The 'how' is recorded in a coherent set of standard agreements ('scheme') on matters such as governance, identification, authentication and authorization (IAA), the cost model, functionality, technology, operation and legal aspects. The agreements apply to every party aiming to share data within or with the energy sector.

Support and inspiration

The development and management of the energy data sharing scheme should primarily be a matter for the parties in the energy sector themselves. To develop a relevant scheme and create a level playing field, it is important that parties with a thorough knowledge of the energy sector develop and take on the governance of the scheme on a joint (i.e. co-creation) basis. This level playing field will gradually bring new parties to the table. A clear model must also be defined for escalation to the regulating authority and the policymakers to resolve any impasses in the future.

Ultimately the energy data sharing scheme could also work in collaboration with other sectors and should support cross-sectoral use cases. That is essential for the implementation of the Climate Agreement. Examples include data exchange between the energy sector and the financial sector for the purpose of mortgage loans to increase the sustainability of residential property, or between the energy sector and mobility sector aimed at pricing transport for EV loading based on overcapacity or undercapacity on the grid. The energy sector can fit in seamlessly in data sharing coalitions, such as the one recently announced by the Dutch Ministry of Economic Affairs and Climate Policy for example.

A new direction

INNOPAY has 20 years of experience with developing such schemes or frameworks all over the world and in a wide range of sectors. We are looking positively and with a great deal of interest at the way in which the energy sector is outlining the initial shape of an energy data scheme. The parties that are currently contributing will have the task of developing it further. Trust in the process and in each other's intentions is very important for this new way of working, and policymakers

have a key role to play. It is important not to define the roles too tightly and to provide the necessary scope and direction in the new Energy Act.

An energy data sharing scheme presents a unique opportunity to move in a new direction and take back control of 'the winner takes most' digital champions – an opportunity to enable the urgently needed Energy Transition in the decades ahead and build an inclusive digital economy. Now is the time to seize it.

Authors

Douwe Lycklama and Maarten Bakker

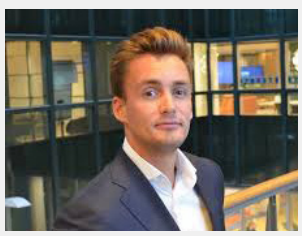
ORIGINAL BLOG

GET IN TOUCH

BLOG

INNOPAY Open Banking Monitor: Banks Moving Beyond the PSD2 Requirements

2 October 2019



Jorgos Tsovilis

Mounaim Cortet

GET IN TOUCH

INNOPAY

In the last few months, Open Banking has seen considerable activity. Indeed, with the EU's compliance deadline for PSD2 looming, Open Banking developer portals have emerged in great numbers, with 300+ banks now in our monitor. Just to name a few newcomers in the Open Banking Monitor (OBM): alBaraka, Binck Bank, Revolut, BPCE Groupe, Santander ES, Commerzbank, Federal Bank, Arab Bank, AKBank, MKB Bank. Several updated developer portals are: ABN-AMRO, Allied Irish Bank, BBVA, Citibank, DBS, Erste Bank, National Bank of Greece, Nationwide, OCBC, Royal Bank of Scotland, Standard Chartered and Swedbank.

In this release of the INNOPAY Open Banking Monitor (OBM), updated in August 2019, we describe the current state-of-play and seek to identify the new Masters in Openness.

Key highlights for banks focusing on PSD2 requirements

The majority of bank developer portals in our OBM consist of EU banks adhering solely to PSD2 requirements (i.e. 76%). More than 250 banks operating in the EU have recently launched their PSD2 developer portal and APIs, consisting of functionalities pertaining to Payment Initiation, Account Information, and Confirmation of Available Funds.

Usually, banks' PSD2 implementation adheres to one of the major API market initiatives (e.g. Berlin Group with 65%), however, some take a proprietary approach to their API specification (i.e. 16%). While PSD2-banks slightly differ in the scope of the PSD2 functionalities offered (driven by the capabilities in their online customer channels) and the API market initiative standards that they apply, these banks mainly differ between each other in terms of Developer Experience (i.e. tools offered by banks in order to connect and understand the APIs).

Banks adhering solely to PSD2 requirements have not been visualised in the OBM. The OBM visual in figure 1 below includes players that have moved beyond this by expanding past the mandatory PSD2 API scope, and frontrunning banks across the world that released new and previously unseen API functionalities. The latter include, for example, Artificial Intelligence empowered accounts information API (by OP-financial). These banks have taken it upon them to provide (potential) API consumers with better engagement tools.

Most PSD2-banks focus primarily on providing only the necessary technical details of the API Documentation and basic Developer Usability tools (see two of the four core developer portal capabilities of the Open Banking Monitor, elaborated in our previous whitepaper on 'How the "Masters of Openness" create value'), allowing visitors to test the available API functionalities. However, these banks lack additional developer guidance, showing a developer where they can find the necessary information and how to connect to a particular API. This is why the majority of PSD2-banks score below average when comparing them to banks from around the world with an Open Banking offering beyond PSD2 mandatory APIs.

A large number of PSD2-banks (i.e. 44%) deploy their offering through so-called 'API Hubs', which provide a single interface to access all banks using their solution. This means that the Developer Experience for banks that make use of the same API Hub can be considered rather similar. Currently, the top three largest API hubs measured by the number of connected banks are BEC (i.e. 23 banks), Luxhub (i.e. 19 banks), and SIBS API market (i.e. 18 banks).

Although many PSD2-banks have launched their developer portal, only 51% indicate that their production APIs are ready for usage. The remaining banks solely provide a sandbox environment with example (customer) data. This example data is generated by the bank in order to mimic what the actual production API will return as output and allows developers

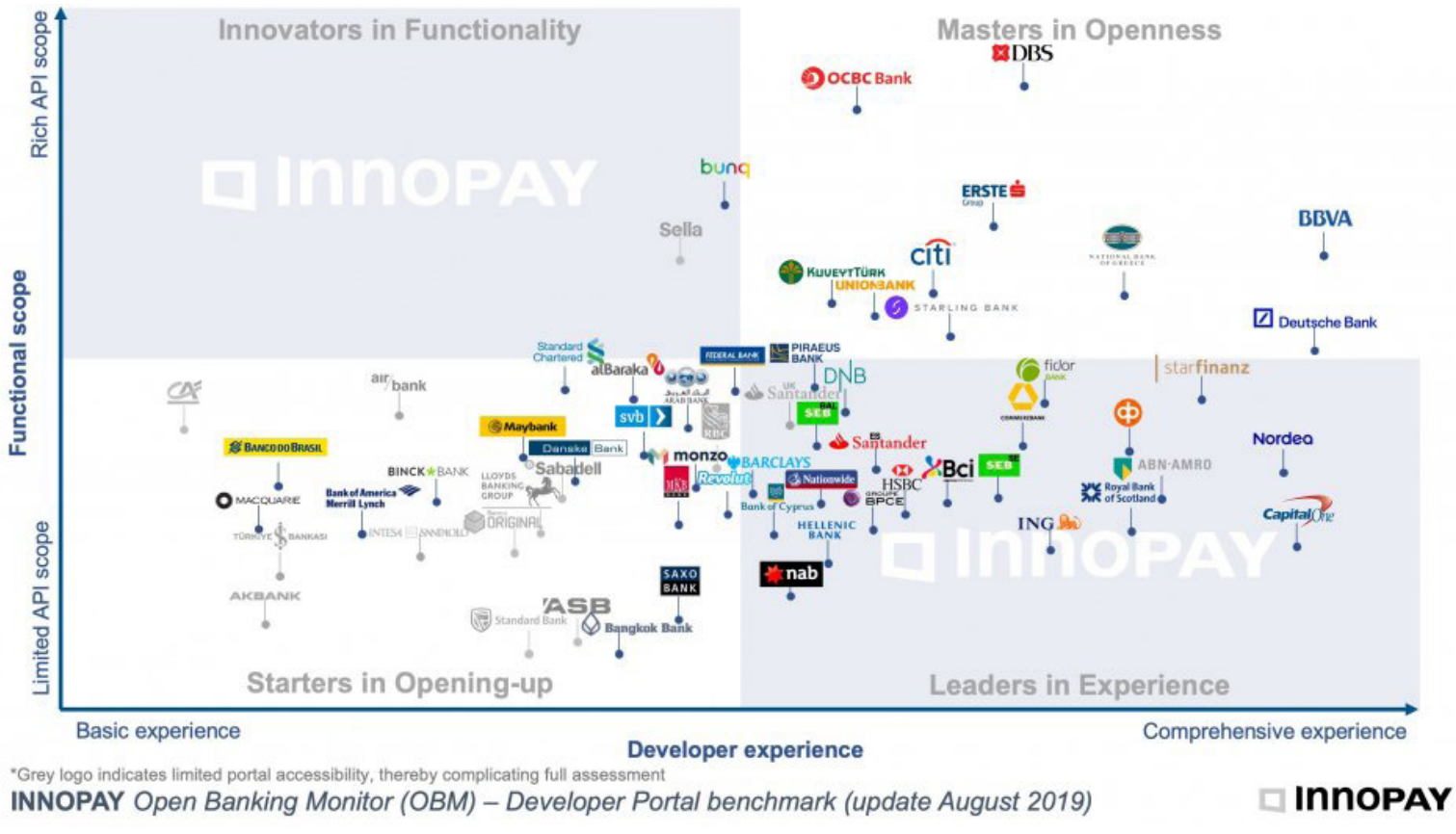


Figure 1: INNOPAY Open Banking Monitor - update August 2019

to test a variety of scenarios. Furthermore, access to the sandbox environment ensures that developers can adapt their implementation to fit the bank's API specifications and test full end-to-end user experience flows. This is why it is interesting that a significant number of PSD2-banks (34%) require a TPP license before developers are allowed to access the sandbox-testing environment, thus prohibiting developers from testing potential use-cases before going through the puzzle of obtaining a PSD2 license.

Key highlights of front running banks in the API economy

Deutsche Bank and **Capital One** have seen a steady performance throughout the past year and together with **BBVA** and **Nordea** now make up for the leaders in Developer Experience. **Deutsche Bank** provides a well-rounded Developer Portal, tailored to both business and developer minded visitors. **Capital One** has clear API Documentation providing all of the necessary components that contribute to a solid documentation and, additionally, actively supports community engagement by ensuring the means to contribute and consume community developed tools.
Several examples are 'Hydrograph', which is a next-generation data integration tool aimed at managing and processing big data, and 'Hygieia', a configurable, dashboard to visualise near real-time status of an entire software delivery pipeline).

ERSTE Group maintains a solid position thanks to their comprehensive app management capabilities, which allows organisations to manage their members and assign them with different roles depending on their access rights, all the while additionally providing means for compliance checks and uploading PSD2 certificates. **HSBC** has recently released a considerable update to their Developer Portal, now delivering a solid Developer Experience with possibilities for API testing and PSD2 APIs for three market API standard initiatives – OBIE, STET, and Berlin Group – something which is not common across other banks.

OCBC and **DBS** continue to grow their API offering with **OCBC**, now offering eight different payment methods. **Bunq** has come a long way, being the third runner up for 'Functional scope', a great performance considering their limited product offering but high granularity of API functionalities. This provides developers with access to virtually every option in Bunq's product portfolio and although it is a small bank, other banks can still learn greatly from this example of what it means to be a truly 'Open Bank'.

Open banking: best practices to shape your API and developer portal roadmap

To support banks who are starting with opening-up or those that are seeking to take the next step in their Open Banking journey, we have identified three key takeaways that could help create focus in their API and developer portal roadmap.

1. **Comprehensible APIs for a broad spectrum of visitors (i.e. business and tech)**

While Developer Portals were initially designed solely for a developer to understand the technical specifications and how to connect to a particular API, an increasing number of banks are now catering for a wider public on their Developer Portals. The visual below shows four elements that can make your developer portal more business-focused.

High-level descriptions, API features, data exposed and potential use cases are all focused on promoting the value the bank APIs provide. This is to ensure that it spikes the interest of the more business-minded visitors as well as the technical developers looking for new and interesting ideas.

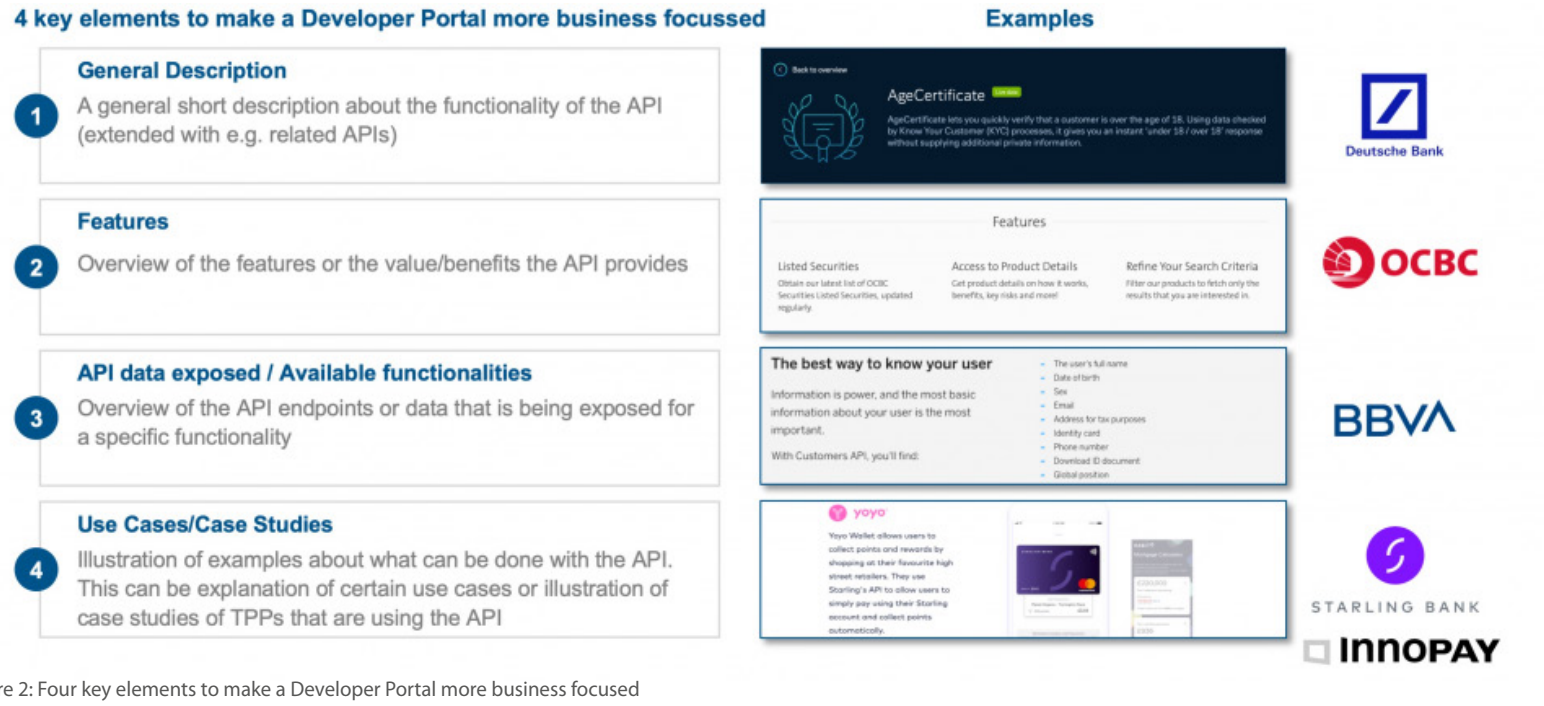


Figure 2: Four key elements to make a Developer Portal more business focused

2. Match the stages of developer interaction to gradual developer onboarding

Six stages can be distinguished in developer interaction and developer onboarding. These stages are depicted in the visual below. Banks need to carefully consider the design of these six stages to ensure a seamless developer experience. Visitors of a Developer Portal first have to explore and see what they can access or use before starting any form of commitment. This is why banks should allow a visitor to quickly browse through the available functionalities and promote the available APIs. Once the visitor has seen enough potential in a particular API, it is time to experiment.

To support this, the bank should provide a sandbox environment, which is easily accessible and handles an ample amount of test data and availability of mock credentials. This will allow developers to understand the user experience flows and identify potential blocking issues for their application. Only once a visitor has requested access to go-live, the bank should connect and start its due diligence and the identification process of the requesting party.

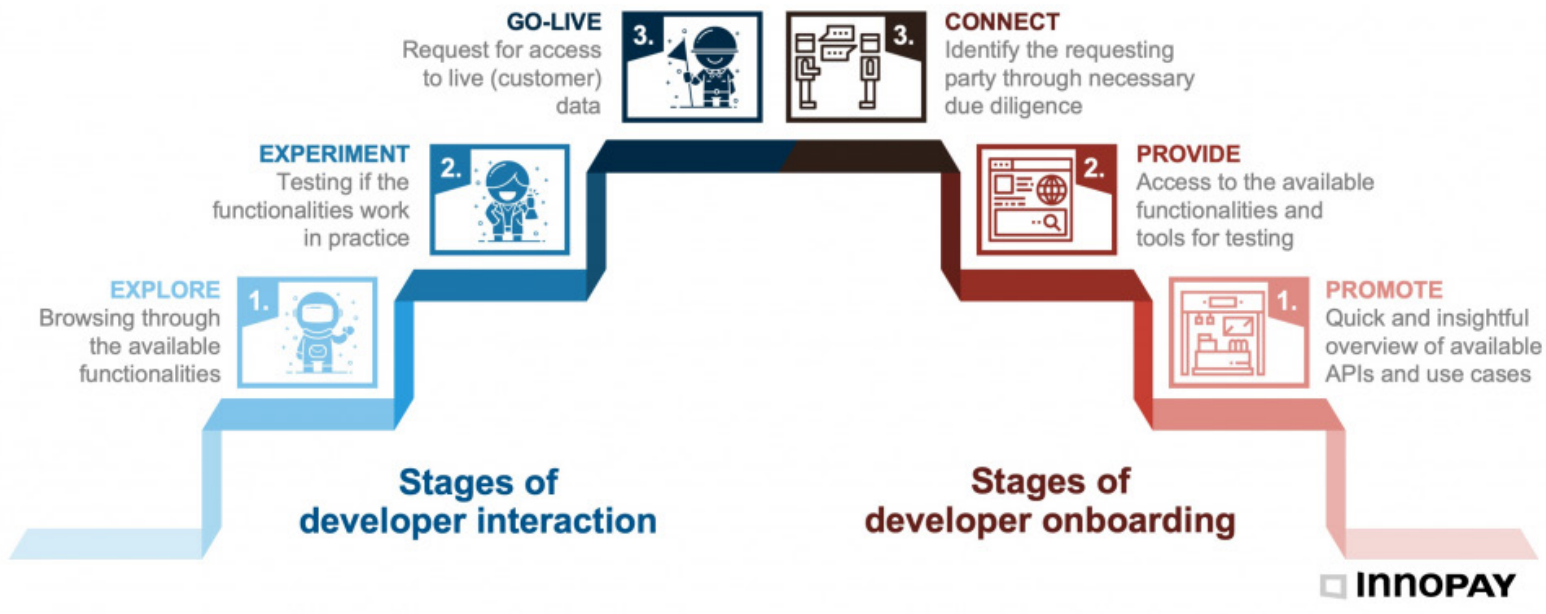


Figure 3: Six stages of developer interaction and onboarding

3. Support Community Development

Community development consists of two related activities in which banks create traction and then promote engagement, and is depicted in the visual below.

A part of Community Development is aimed at 'creating traction' around the bank's Open Banking offering. This means actively advertising and promoting activities such as Open Banking events, hackathons or updates to the portal, newsletters, blogs or other channels. However, perhaps equally important in order to maintain traction is 'promoting engagement'. Examples of banks that do this well are **Capital One** – with their 'Open source first approach', in which they actively use, contribute, and manage open source software projects and allow the community to contribute as well. **Starling Bank** is another example, by creating a marketplace exposing all the financial products developed by third parties that consume Starling's APIs. This helps new developers to get started on their own projects by using ready-made pieces, triggers visitors with potential ideas and use cases, and shows the bank's customers what added (banking) functionalities are out there which they can use and experience.

Open Banking is heading towards a state in which banks aim to involve the community as much as possible, allowing them to contribute by providing the necessary tools and promoting their engagement. This creates an immortal state in which the bank profits from community-created content that, in turn, sparks others with new and innovative ideas.

Reach out to discuss the opportunities if you are starting your Open Banking transformation and/or when you are seeking to take the next step in your Open Banking journey. Stay tuned for more updates of the INNOPAY Open Banking Monitor.

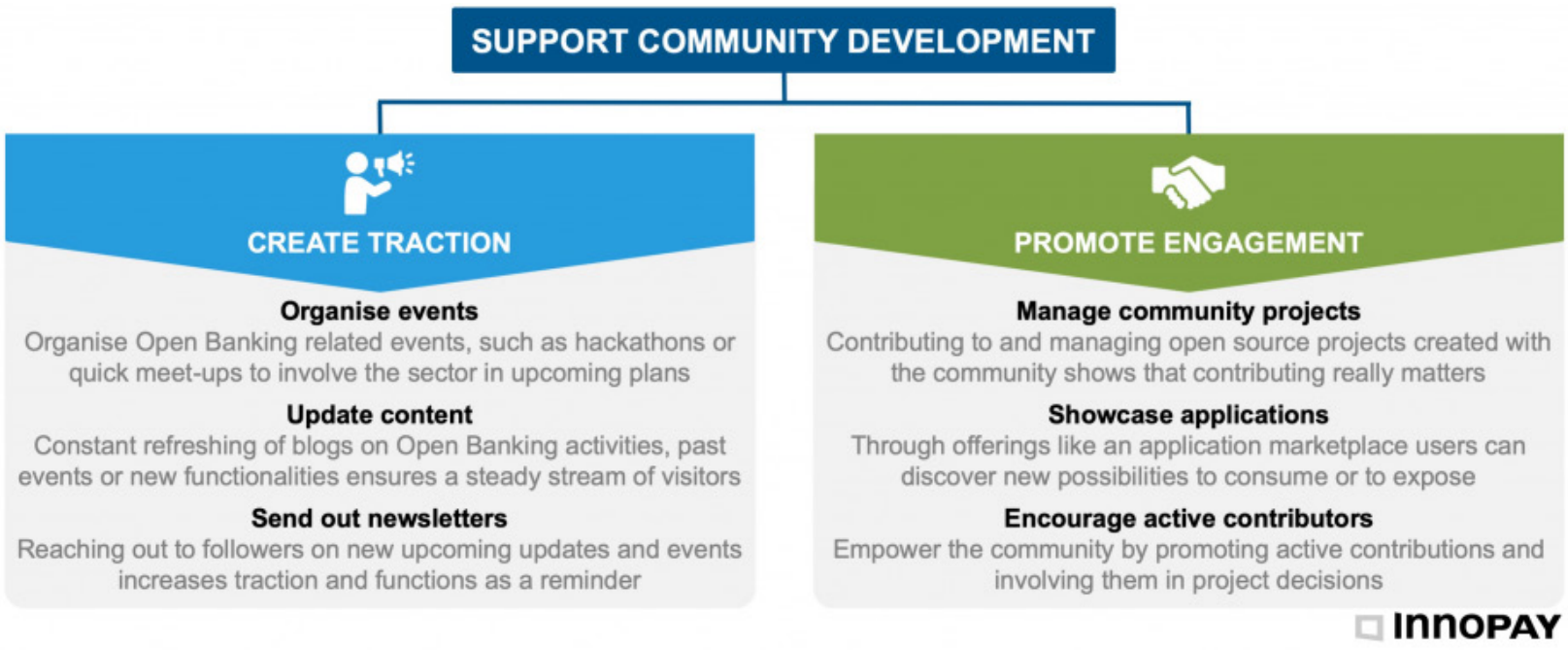


Figure 4: Community development support activities

Authors

Jorgos Tsovilis and Mounaim Cortet

ORIGINAL BLOG

GET IN TOUCH

BLOG

Open banking is the start of something much bigger: an Open Data economy

7 October 2019

Innovations are happening faster than ever in the world of payments and data, driven by a major trend towards providing consumers increasing control of their data. According to Vincent Jansen, Partner at INNOPAY, and his colleague Mounaim Cortet, head of Open Banking, Open Banking is actually the start of something much bigger: an Open Data economy.

Open data economy as a basis for data sharing

To move from Open Banking to an Open Data economy, we first need to understand that an Open Data economy gives consumers full control of their personal data. They own it and have the tools to specify with whom they are willing to share particular data, what those parties are allowed to do with it and for how long. Jansen and Cortet believe that it should be a human right to control and grant others access to your own data. That would support a shift towards a more equal 'data benefit balance' as described in the Dutch management book of the year, 'Alles Transactie' or 'Everything Transaction'. Then, not only major companies but also consumers would be able to exploit the benefits generated from their data.

More control of your own payment data

Cortet sees Open Banking as the first step towards the Open Data economy. Open Banking describes an ecosystem in which banks increasingly open up their systems. Whereas payment data used to be controlled exclusively by the banks, that control is

GET IN TOUCH

INNOPAY

increasingly shifting to the consumer. PSD2, the new European payments directive, is being implemented to accelerate this process. It gives consumers the right to authorise third parties to access their payment data. They can also give these parties consent to initiate payments on their behalf. The empowerment of consumers to control their data is therefore no longer a theoretical concept but is actually being implemented in practice.

INNOPAY's Open Banking Monitor shows that banks are gradually opening up. It describes a trend whereby banks are increasingly developing from 'starters in opening up' to 'masters in openness' (see Figure 1). It looks first at the extent to which banks are opening up and making data and functionality available to third parties, naturally with the consent of the customer concerned. It also assesses the quality and scope of the resources that banks are providing so other parties can integrate more easily and develop innovative applications for their customers.

Banks have an important role to play

The evolution of banks in the Open Banking ecosystem shows that the ideal of the Open Data economy is not just a hollow phrase but could actually become a reality. Banks not only have an exemplary role but are also very proficient at determining consumers' digital identities due to their Know Your Customer (KYC) obligations. Jansen claims that thanks to these digital identities and strong customer authentication (SCA) mechanisms, banks can already play a key role in giving consumers control of personal data in other sectors. After all, consumers must be identified with sufficient reliability if they are to irrefutably authorise other parties to use particular data.

The mandatory opening up of banks has also enabled them to gain experience in obtaining and managing authorizations from consumers. Each authorization must be recorded securely and reliably, so the consumer always has an up-to-date overview of the parties which have been given access and,

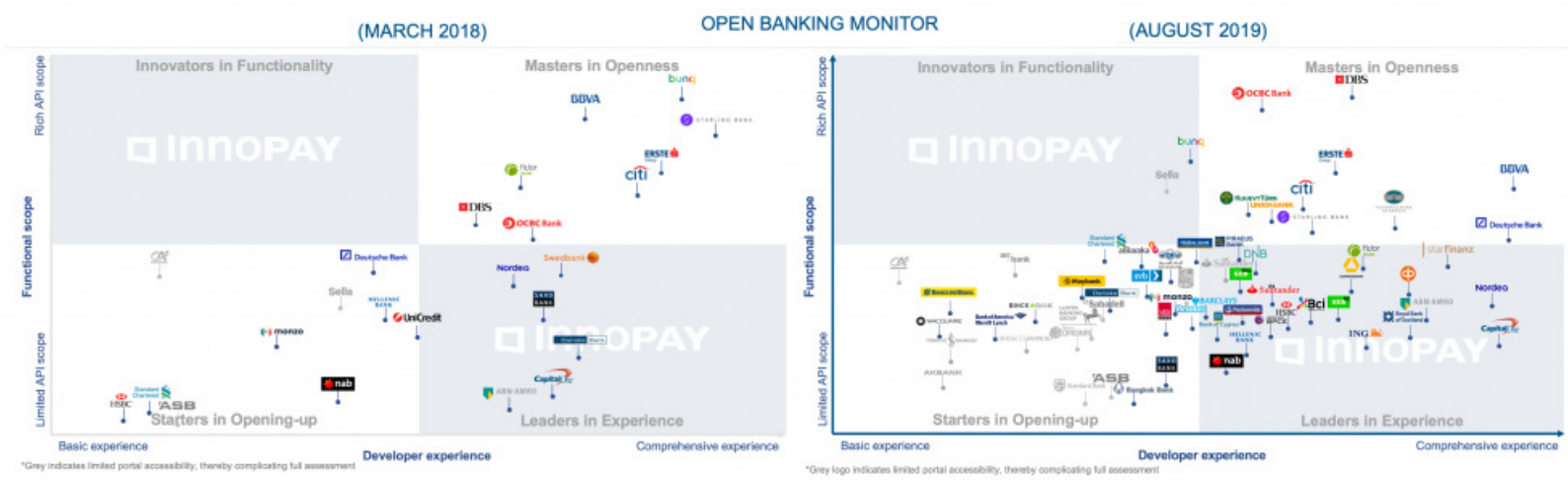


Figure 1. The Open Banking Monitor. Left: March 2018, right: August 2019. © INNOPAY

if desired, can also withdraw that access. This experience, combined with the experience in digital identity, provides an important resource that can be deployed beyond the confines of banking. By turning this experience into services, banks can take a significant step towards facilitating the Open Data economy in other sectors.

National trust infrastructure

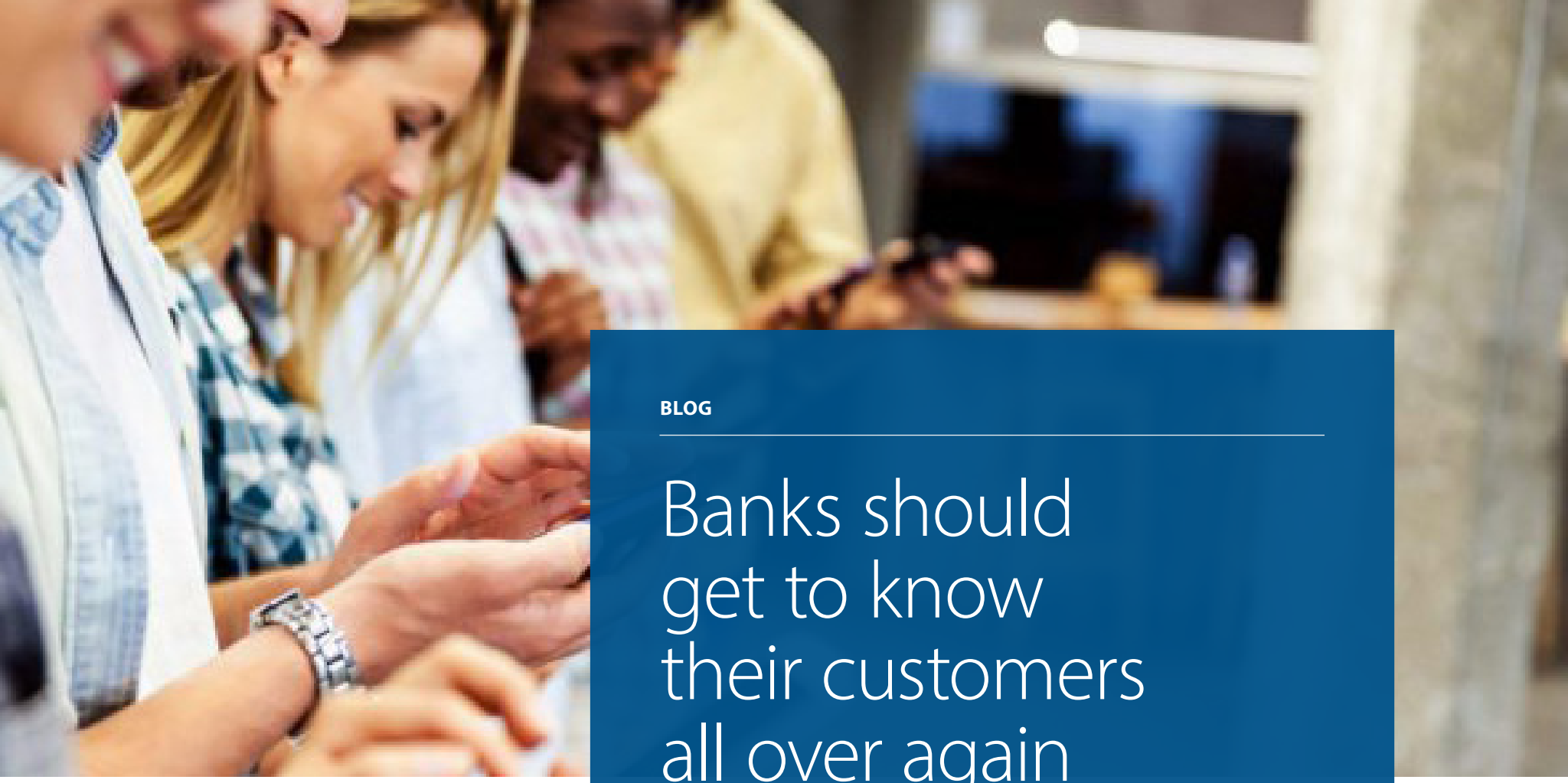
Needless to say, managing and sharing data from a large number of sources requires more than just a digital identity and the management of authorizations. Cortet believes that a national trust infrastructure needs to be created to exchange data. This requires the development of a scheme for data sharing, digital identities and authorizations. Such a scheme is not very different from those used in payments (e.g. Mastercard, VISA). It records the functional, technical, operational, business and legal agreements that are necessary to give consumers control of their data. Such a scheme requires collaboration, initially with banks in the pioneering role thanks to their experience followed by the subsequent involvement of other public and private-sector operators.

Cortet believes that proactive investment in a national trust infrastructure will make legislative intervention unnecessary. The PSD2 provides for the opening up of banks but omits or inadequately addresses a number of key issues, making the rollout difficult in practice. Jansen hopes to see a more market-driven initiative for the national trust infrastructure across various sectors, giving rise to a kind of consumer-branded service for data sharing: a service that all consumers know, trust and use almost daily, to share – and finally reap the benefits of – their own data.

Reach out to Mounaim Cortet or Vincent Jansen to discuss the opportunities if you are starting your Open Banking and Open Data transformation, or when you are seeking to take the next step in your Open Data journey. Stay tuned for more updates on the Open Data economy!

ORIGINAL BLOG

GET IN TOUCH



BLOG

Banks should get to know their customers all over again

8 October 2019

Mariane ter Veen

With the Open Banking initiative now well and truly underway, we're gradually seeing the first signs of banks and banking associations informing the public about what it involves. And this is not a minute too soon, because consumer awareness about Open Banking is still low. According to recent research [1], only 18% to 35% of banking customers would feel comfortable sharing their account information with another bank in exchange for new online services.

For consumers to benefit from Open Banking, it is necessary that banks embrace 'openness' (beyond PSD2) by exposing their assets through APIs, that applications are built on top of those APIs, and that consumers use them – adoption, in short. Consumer education is critical in facilitating adoption. As banks play a central role in Open Banking ecosystems, their approach to educating consumers is key to creating success.

For some, it may sound illogical for banks to play a dominant role in helping customers to use Open Banking services. Surely they risk losing business to third parties? However, the real risk lies in them not doing so. Traditional account services have become a commodity, and it is increasingly difficult to make a profit on such services. Banks have started to recognise that Open Banking opens up new business potential. Banks with an attractive customer base, perfect developer conditions (sandbox, developer portal), and wise monetisation choices will stimulate the use of their APIs, resulting in applications built to help their customers.

GET IN TOUCH

INNOPAY

Maybe even more importantly, many believe that Open Banking is just the start. There are numerous signs that the open data initiative is spreading to other sectors, with new legislation aimed at putting the customer back in control. For example, Australian CDR legislation starts in banking but is intended to expand to energy and telecommunications. Meanwhile, the Dutch Ministry of Health, Welfare and Sports is taking concrete steps towards making electronic data exchange in accordance with the appropriate information standards a statutory obligation. This effort is about sharing data and tipping the 'data benefit balance' in the consumer's favour.

In this endeavour, trust is the essential ingredient for success. For consumers, key questions include 'Do I sufficiently trust the supplying party to provide access and share specific parts of my data in order to receive services that will benefit me?' and 'Who or what is backing up this trust?'. On a practical level, consumers also wondering 'How do I keep track of whom I trust with what?.' For service providers, trust revolves around questions such as 'Do I have enough certainty on this customer to deliver my services?'

Against this backdrop of trust, banks are well-positioned to play a crucial role. There has long been a well-known saying in banking: 'Customers may dislike us, but they trust us.' This captures the sense that banks are regulated and licensed to work with consumers' money and data, but few consumers have a positive emotional connection to their bank's brand. Therefore, before consumers become willing to extend their trust in banks beyond the traditional domain and into new services – services that lie close to their homes, hearts and families – they first need to learn to like their banks all over again. In other words, to capitalise on the opportunities of Open Banking, banks need to change.

At the same time, banks can turn the process of informing consumers about Open Banking into a chance to win back the customer's favour. When it comes to educating consumers, banks have a choice: should they tap into the 'fear' aspect or the 'fun' factor? The first approach focuses mostly on explaining PSD2 and the technical and legal implications for customers. Additionally, it emphasises the risks and the fact that customers do not have to give their consent. In fact, in a letter to inform me about the upcoming PSD2 regulation, my own bank wrote: 'It is important to know that you don't have to open up anything if you don't want to.' This is very much in line with what banks have historically told people: 'Do not share your data or your PIN with anyone; beware of digital scams.'

But in the second approach, banks can reinforce their position as trusted partners. They can highlight how they play a positive role in making it clear and easy for consumers to actively manage their Open Banking consents. They can educate their customers about the benefits of Open Banking: how consumers can become financially savvy, get the most out of their money and data, and make use of new and innovative payment methods. Banks can also provide guidance to consumers in terms of what they should look for in services and what they can do if something goes wrong. They could even truly open up to their customers and allow them to rate the Open Banking services provided. In my opinion, the choice is clear: banks should put the 'fun' back into finance when educating consumers about Open Banking, and proudly present themselves to customers in their new, trusted and liked role.

1. Deloitte's CEE PSD2 Voice of the Customer Survey, Jan. 2018

Author

Mariane ter Veen

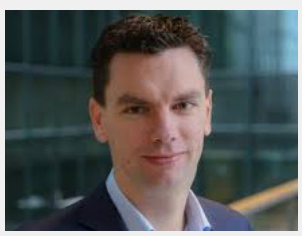
ORIGINAL BLOG

GET IN TOUCH

BLOG

PSD2 and Open Banking Use Cases for Insurers in an Open Data Economy

10 October 2019



Maarten Bakker

Mounaim Cortet

Vincent de Rijke

GET IN TOUCH

Legal drivers such as GDPR and PSD2 in Europe and CDR in Australia are enabling the customer with more ownership and control over its own data. As a result, the customer is increasingly empowered to more easily provide consent-based access to his/her data by a service provider of choice. This trend is accelerating across countries, industries, and market actors and as such we are moving towards an Open Data economy. In this emerging landscape, data is shared between organisations under control of the rightful owner(s) and used by third parties to improve or develop new business models and service concepts.

This increased availability of data in new ways brings insurers new opportunities to build or improve risk models and develop new products and services. As an initial step, insurers can already start capitalising on the Open Data economy by exploring useful use cases that will become available under PSD2 (XS2A) and Open Banking.

Access to account (XS2A) under PSD2 provides opportunities to insurers

One major development contributing to concrete customer ownership and control over data is visible in the European financial sector, where PSD2 enables customers to allow a third-party access to their payment account (XS2A). Based on a customer's consent, the third party can retrieve account information from a customers' payment account (covering balances and transaction history) or initiate payments from a customer's payment account.

Open banking enables additional possibilities for insurers

A visible trend in the emerging PSD2 ecosystem is banks opening up data and functionality beyond XS2A, such as information on other account types, customer's identity data and aggregated and anonymised information on their customer base. The INNOPAY Open Banking Monitor provides a comprehensive overview of the masters in openness that move beyond mere regulatory compliance. Again, here, all access to these data and resources is based on a customer's consent. The data and functionality that become available - as a result of the trend towards openness in banking - enable beneficial use cases for insurers, across their traditional value chain and beyond. Potential use cases are summarised in figure 1.

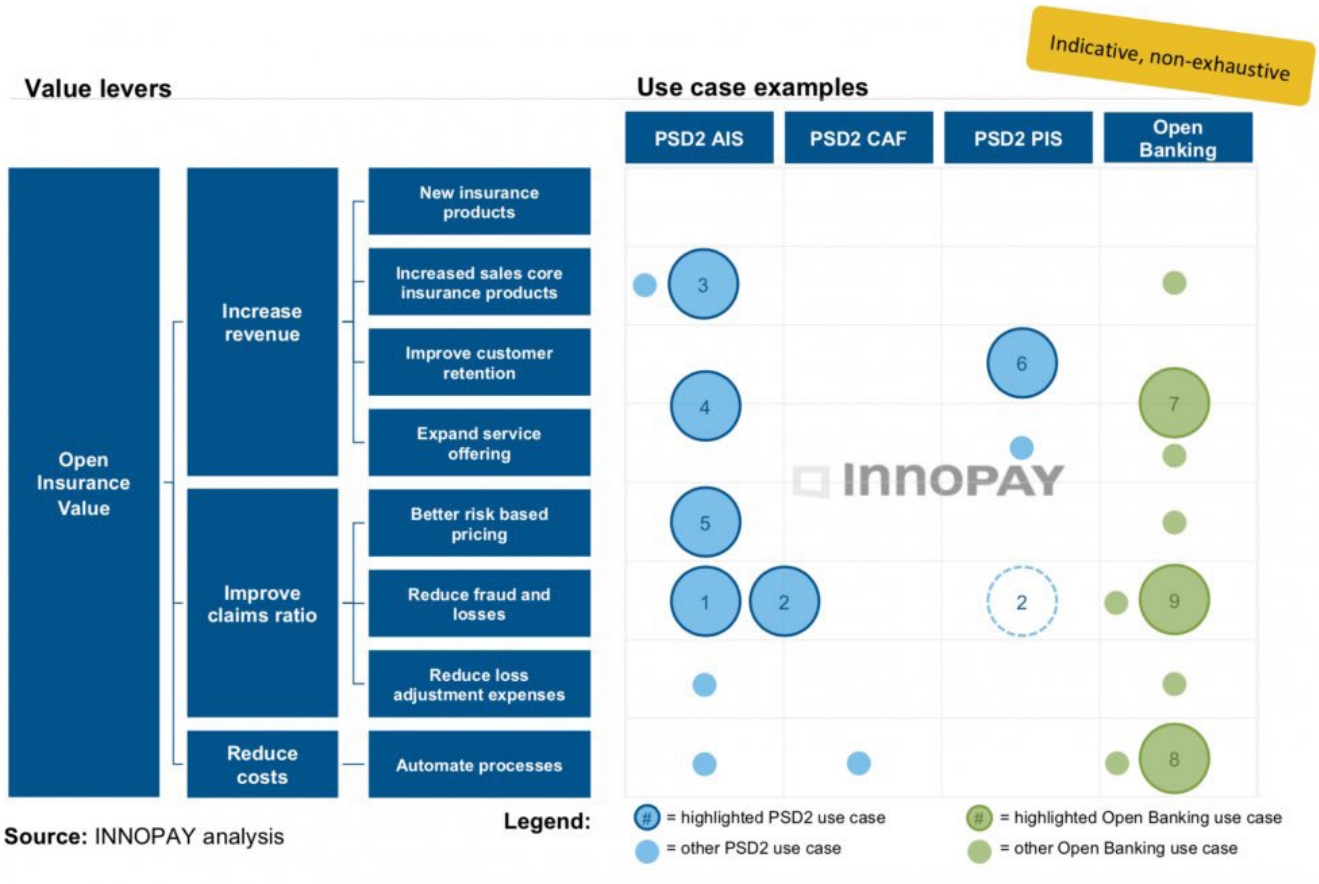


Figure 1: use cases across the insurance value driver model, based on the level of customer data that is needed to realise the use case

In the section below a selected set of nine use cases are explained in further detail.

Examples of use cases for insurers based on data and functionality in the scope of PSD2 XS2A

Some selected use cases based on functionality available under PSD2 XS2A are:

1. IBAN-name check

An IBAN-name check helps to reduce fraud with improved potential of checking accountholder authenticity, and reduces the number of corrective money transfers needed due to incorrectly registered IBAN;

2. Improved debit collection process:

Account balance checks before initiating payment (direct debit) requests, reduce bounced requests. Furthermore, through payment initiation, the insurer has the opportunity to provide personalised reminders to pay, decreasing the costs of debtor management;

3. Improved acceptance process:

As account data enables next-level risk-profiling, it can prove to be of assistance in a faster and improved, or even automated, acceptance of customers;

4. Personalised financial advice

Account data enables in-depth insights in spending patterns and a customer's financial position that can be used to provide personalised financial advice;

5. Personalised or dynamic premium quotes

Risk-profiling based on account data enables strategies and tools for personalised premium quotes;

6. Additional payment methods

Offering an alternative to traditional direct debits for premium payments and (ad-hoc) payments for services, as some insurers are transitioning from being a mere insurer towards a service provider that foresees in the customer's needs at the point of relevance.

Examples of use cases for insurers based on open banking data and functionality

More functionalities and customer data become available as banks venture into the Open Banking play. Three highlighted use cases (based on data and functionality that are currently opened up by a subset of banks) that can bring specific value to insurers are described below:

7. Improved personal financial management services

Insurance companies offering personal financial management applications can include a function to retrieve all accounts (e.g. accounts related to savings, credit cards, mortgage, pension, investments) at once;

8. Retrieve up-to-date user address

Since customers are usually more inclined to update their address in a timely fashion at their bank, insurers can facilitate the customer by checking the last known address at the bank;

9. Verify customer ID

Insurers can raise barriers to cases of identity fraud by including banks' API identification functionalities in the insurance onboarding process.

Key success factors in exploring new business models for PSD2 and open banking

The data and functionality that will become available provide a wide array of opportunities for insurers. While insurers are well-positioned to act on these opportunities, there are some key success factors to consider.

First, insurers need to enable secure and cost-effective API connectivity with banks. It is key to select the right service provider that can offer this connectivity 'as a service' in order to contribute to your requirements and strategic objective.

Second, insurers should think about a clear and transparent consent strategy. Customers must be fully aware of the data they are sharing and the purpose for which it is being used. Safeguarding the data benefit balance is of utmost importance to persuade customers to share their data.

Third, once the necessary data is retrieved with the consent of the customer, it needs to be 'crunched'. There is a need for solid data analytics capabilities to mould the data into customised and personalised (financial) advice for customers.

Sharing data is a new phenomenon and the opportunities present new fuel to establish relevance and possibilities for differentiation. Insurers that put in place a solid strategy for an Open Data economy will be in a good position to seize the opportunities brought forward by PSD2, Open Banking and the Open Data economy at large.

Authors

Maarten Bakker, Mounaim Cortet and Vincent de Rijke

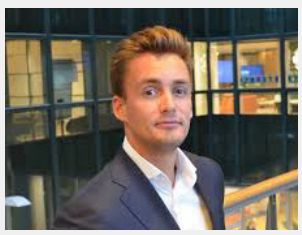
ORIGINAL BLOG

GET IN TOUCH

BLOG

How can crypto service providers prepare for the rapidly approaching AMLD5 requirements?

2 October 2019



Jorgos Tsovilis

Mounaim Cortet

GET IN TOUCH

INNOPAY

The EU's fifth Anti Money Laundering Directive (AMLD5) comes into force in all Member States on 10 January 2020. This latest version of the directive broadens its regulatory scope by including two types of crypto service providers (CSP): virtual-fiat exchanges and custodian wallet providers. The main driver behind this regulatory update is to decrease anonymity in crypto transactions and hence combat money laundering and the financing of terrorism. The change in the regulation confronts CSPs with three main uncertainties that need careful consideration… and with the deadline rapidly approaching, there is not much time left. Read this blog to learn how to start preparing your client- and internal processes before it is too late.

Generally speaking, CSPs are not used to being regulated. Many will find it challenging to demonstrate regulatory compliance whilst ensuring optimal continuity of their activities. The difficulty of this task is mainly due to the following three uncertainties:

- the applicable regulatory scope and definition of CSPs
- diverging regulatory procedures and requirements between countries
- how to design compliant, risk-based Customer Due Diligence (CDD) procedures whilst minimising client impact.

As the first in a series of blogs, this article aims to help existing and prospective CSPs with understanding and managing these uncertainties, and with proving their

compliance to regulators whilst continuing their activities with the minimum of disruption. But first, let's remind ourselves of the recent crypto market developments.

As the crypto market has matured, regulators have responded

The crypto asset ecosystem has undergone significant changes. The aggregate market capitalisation of global crypto assets skyrocketed from around EUR 30 billion in April 2017 to more than EUR 700 billion at its peak in early January 2018, until coming down again to hover at around EUR 200 billion [1]. The industry was confronted with massive inflows of new users and funds. This has led to the emergence of additional service providers such as crypto exchanges, wallet providers and brokers. The broader application of crypto assets, combined with its unregulated status and relative anonymity, increased the risk of crypto assets being used for financial crime.

Regulators around the world have responded to these newly emerging risks by introducing new regulations. The AMLD5 [2] is part of the European Commission's anti-money laundering and anti-terrorism efforts, aimed at increasing transparency (e.g. national UBO registers) and expanding its reach (e.g. prepaid cards, specific CSPs). AMLD5 is the first European Union (EU) legislation which provides a legal definition for the term 'virtual currency'. Due to its multi-interpretability, however, this definition is already being widely debated [3]. For both CSPs and regulators, this makes it difficult to determine which requirements apply in certain cases.

Uncertainty around the applicable regulatory scope and definitions of csp

Depending on the exact business model and activities of a CSP, different authorisation (i.e. registration or licence) requirements may apply. If CSPs are uncertain about the requirements for their specific activity, they can reach out to the regulator in their home country. This will prevent them from unexpectedly having to cease their crypto activities later on. In the EU we mainly see three forms of legal classifications of crypto asset activities which require an authorisation from a regulatory authority:

1. **E-money,**

which is broadly defined as 'electronically/magnetically stored monetary value as represented by a claim on the issuer, which is accepted as a payment method by parties other than the issuer' and requires an e-money institution licence under E MD2 [4]

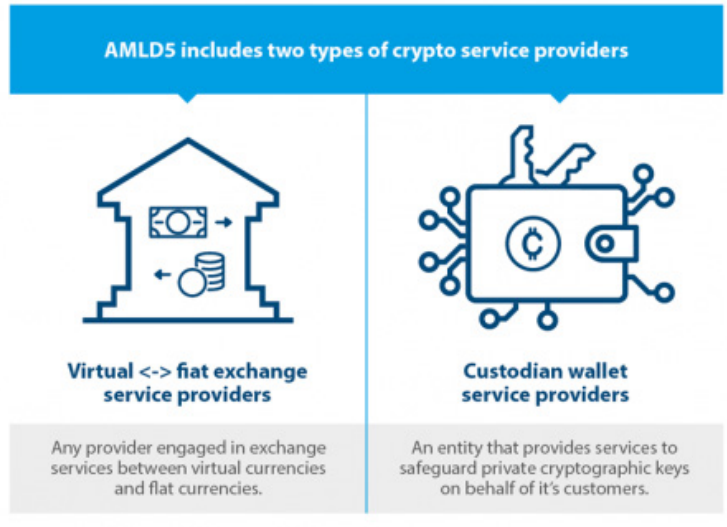
2. **Financial instruments,**

as it is sometimes argued that investors treat crypto assets as a substitute for financial instruments such as securities trading, which requires an investment firm licence under MIFID2 [5]

3. **Virtual currencies,**

which are broadly defined as 'a digital representation of value that is not issued or guaranteed by a central bank or public authority and is accepted as means of exchange' and where two specific CSPs require a registration under AMLD5.

Two specific types of CSPs have been added in AMLD5: virtual-fiat exchanges and custodian wallet providers (for definitions, see Figure 1).



Two examples of virtual-fiat exchanges are Binance and Bitonic. A custodian wallet service provider, such as Bitvavo or Freewallet, controls the user's private keys and is in full control of the customer's funds. Wallet providers who do not control the user's private keys currently remain beyond the scope of AMLD5 because they cannot access the user's funds in any way. This limits their ability to comply with AMLD5 rules such as transaction monitoring.

If CSPs fall under either of these two definitions, they need to comply with the AMLD5 requirements before 10 January 2020 and obtain a registration at the regulatory authority in each of the EU countries in which they operate. Passporting, a regulatory practice which allows firms registered in the EU to do business in other Member States without need for further authorisation, is not possible for the AMLD5 registration.

Uncertainty around diverging regulatory procedures and requirements between countries

All CSPs with activities that fall under the three above-mentioned crypto asset classifications (e-money, financial instruments and virtual currencies) must comply with the AMLD5 requirements, which are broadly summarised and visualised in Figure 2.

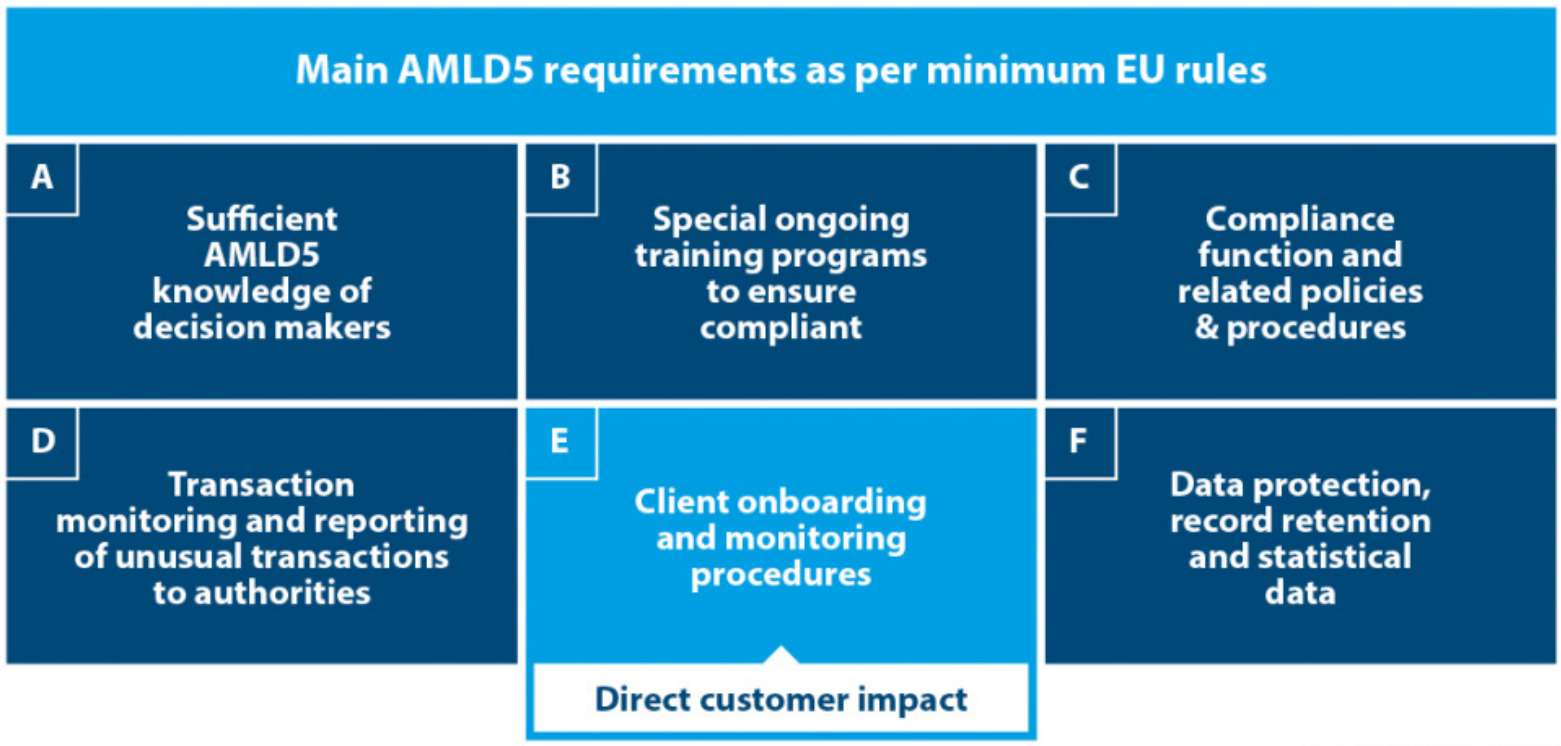


Figure 2: Main AMLD5 requirements for regulated players as per minimum EU rules.
Individual countries may impose stricter requirements due to different interpretations.

This confronts CSPs with another uncertainty and complicating factor. In principle, AMLD5 aims to harmonise the requirements for CSPs across the EU, but individual Member States may interpret the requirements differently as the AMLD5 is transposed into national legislation, resulting in differences between countries. Current examples of deviating requirements are in Lithuania, where crypto-crypto exchanges are also expected to be in the scope (as opposed to only crypto-fiat exchanges) [6] and in The Netherlands, where the board members (day-to-day policymakers) of the entity need to be approved before a registration can be obtained [7]. As not all supervisors have published their approach towards authorisations yet, CSPs should keep a close eye on the developments to determine the organisational impact of the requirements.

Uncertainty around how to design compliant, risk-based customer due diligence (cdd) procedures whilst minimising client impact

Achieving and maintaining compliance on the above-mentioned topics not only affects the internal organisation, but also directly affects customers. Since AMLD5 aims to reduce the risk of money laundering and terrorist financing, CSPs are required to conduct Customer Due Diligence. This means that they need to collect and verify information about who their customer is, perform a risk assessment before the customer is accepted and subsequently monitor customers and their transactions. These requirements are at odds with the relative anonymity that customers currently enjoy. As a result, CSPs are required to substantially change their customer onboarding and monitoring processes. Inadequate design of these processes can negatively impact a CSP's business by harming conversion rates. Even seasoned financial institutions such as traditional banks struggle to comply with these strict rules, so these processes need to be designed with due care.

Digital onboarding and monitoring requirements imply that CSPs need to obtain and monitor identity-related attributes from the customer, but the specific requirements may vary per country. Furthermore, it is not specified how these attributes should be obtained and verified, because the regulations aim to remain technology agnostic [8] and advocate a risk-based approach. This gives you room to design your customer journey as you see fit, but also leads to uncertainties on how to

determine the risk-associated and design-compliant processes, especially as CSPs have limited experience in doing so. To help CSPs with this challenge, Figure 3 summarises the process for designing compliant and risk-based onboarding and monitoring procedures.

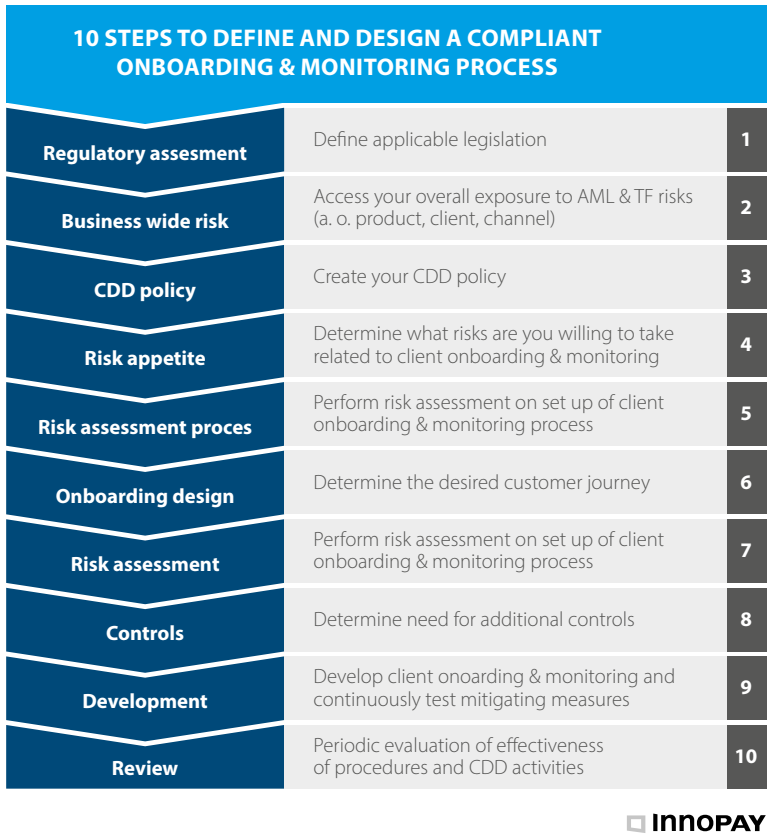


Figure 3: 10 steps to define and design a compliant onboarding & monitoring process

Conclusion

To summarise, this blog discusses three main uncertainties around achieving and maintaining AMLD5 compliance as a CSP:

- Do you fall within the scope of the AMLD5 and which authorisations do you need?
- Which (local) regulatory requirements exist and what is the impact on your operating model?
- How can you ensure a compliant approach on key processes such as customer onboarding and monitoring, whilst minimising the effect on your customers?

Since not all local legislation and supervisory approaches are final or publicly available yet, CSPs are advised to keep a close eye on these market developments to determine how to demonstrate their compliance to regulators whilst ensuring optimal continuity of their activities. INNOPAY can help CSPs with all these challenges. If you are looking for best practices, expertise on regulatory requirements and their impact on your operating model, or support with authorisation procedures with your respective supervisor, please feel free to contact Josje Fiolet and/or Tycho van Ewijk.

1. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-12-ccaf-2nd-global-cryptoasset-benchmarking.pdf

2. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

3. https://paytechlaw.com/en/new-legal-definition-amld5/

4. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32009L0110

5. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0065

6. https://news.bitcoin.com/lithuania-to-adopt-crypto-regulations-even-stricter-than-the-eus/

7. See item no. 7, as part of a published FAQ by the Dutch Central Bank: https://www.toezicht.dnb.nl/en/2/50-237833.jsp

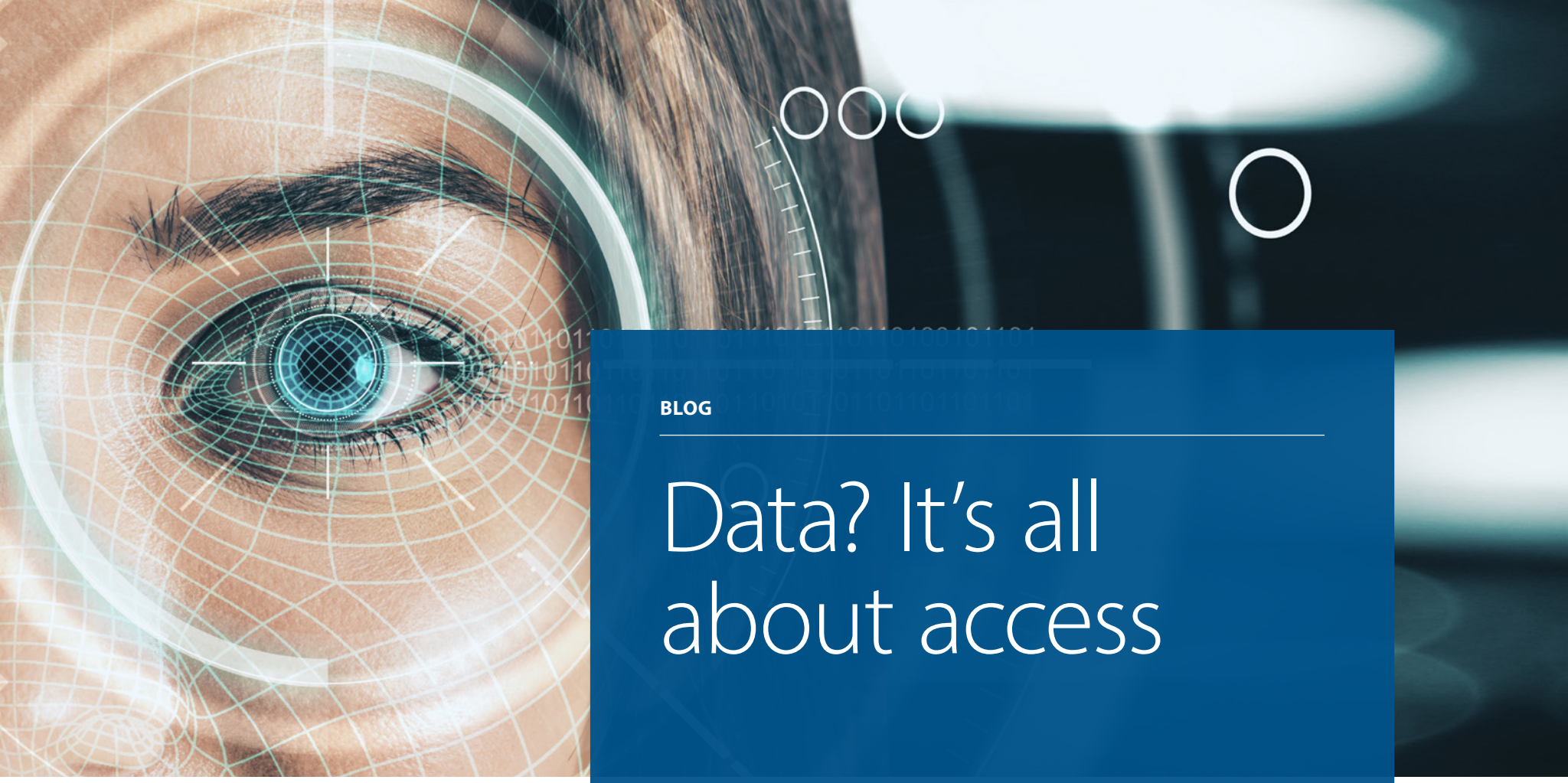
8. Some exceptions may apply, for example in Germany where the BaFin prescribed the use of video technology for digital identification

Authors

Jorgos Tsovilis and Mounaim Cortet

ORIGINAL BLOG

GET IN TOUCH



BLOG

Data? It's all about access

11 November 2019

Mariane ter Veen

Everybody seems to be talking about data these days – either about the 'cool stuff' you can you do with it, linked to buzzwords such as blockchain, artificial intelligence (AI) and 'big data', or about data itself: data quality, data sharing, data leaks and data security. But it strikes me that there's a gaping hole in these conversations: access to data. As we increasingly move towards the transactional era, this apparent collective lack of interest in managing data access is starting to cause serious problems.

Apart from scientists and policymakers, most people haven't tended to care about data access and have so far been sharing their data willingly. Many regard it as 'a price you have to pay'; if you want to stay connected through social media and want the convenience of ordering online, you go ahead and click on "I agree". However, people are becoming increasingly aware of the fact that they subsequently have no control over the data they provide. The realisation is slowly dawning that others – usually the tech giants such as Facebook, Google, Amazon, etc. – are using people's data for their own benefit, yet giving nothing (or very little) in return.

In the EU we have the GDPR data protection and privacy directive, of course, but it still doesn't provide a real means to express the rights we have over our own data. We lack data sovereignty, we lack the ability to decide who can do what with our data under what conditions – in other words, we lack control over our data. And it's all because we don't have the right focus: a focus on data access.

GET IN TOUCH

INNOPAY

Rising to the challenge and tackling the risks

This affects not only consumers, but also organisations. Because there is no way organisations can provide access to their data in a controlled, standard and easy way, many of them decide not to share data at all. In the Dutch healthcare sector, for example, organisations stopped sharing data about the results of mental health treatment due to new regulations that were actually meant to protect user rights. Regulation turns into an excuse to not share data. This has prevented health institutions from gathering essential data on the effectiveness of mental health treatment for the past three years.

The lack of focus on data access is also hampering innovation across the board. Just imagine how much more could be achieved in sectors such as healthcare, logistics and energy if data sharing could be made seamless and secure.

To rise to these challenges and tackle the risks, we require access to sufficient high-quality, relevant and unbiased data, including the necessary rights to use it. People need to be able to manage the access to their data – to regain control. Only then will we be able to restore the 'data benefit balance' and help our data economy thrive. But first, we need to have the right discussion.

How INNOPAY's triple a model facilitates the data access discussion

To those organisations who are keen to help change the mindset towards data access, I'd like to propose the INNOPAY Triple A model. This model visualises the data issue as comprising three layers: Availability, Access and Application. It is built on the principle that data availability and data access are preconditions for any data application. When data becomes separated from applications, an access layer or exchange layer is needed.

This 'soft' infrastructure could serve as the basis for control and enable sound data sharing, just as hard infrastructure (such as waterways, roads, railways, sewers and the electrical grid) has been the foundation of health, wealth and economic growth from the time of early civilisations. In other words, the access layer is the infrastructure that will help to build a solid and sustainable foundation for the next growth cycle of the digital data-driven economy.

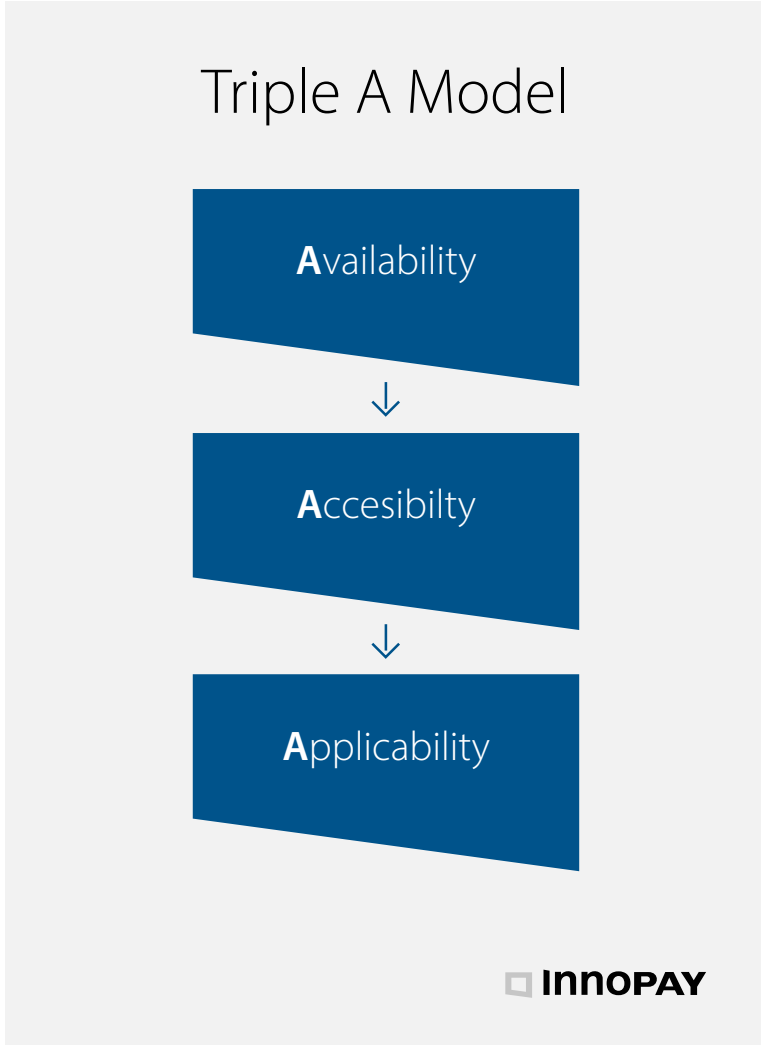


Figure 1

The central design principle of this soft infrastructure should be data sovereignty: giving organisations and people alike the possibility to control what's happening with their data.

A common vision and shared standards are crucial to adoption, so this must be coordinated carefully.

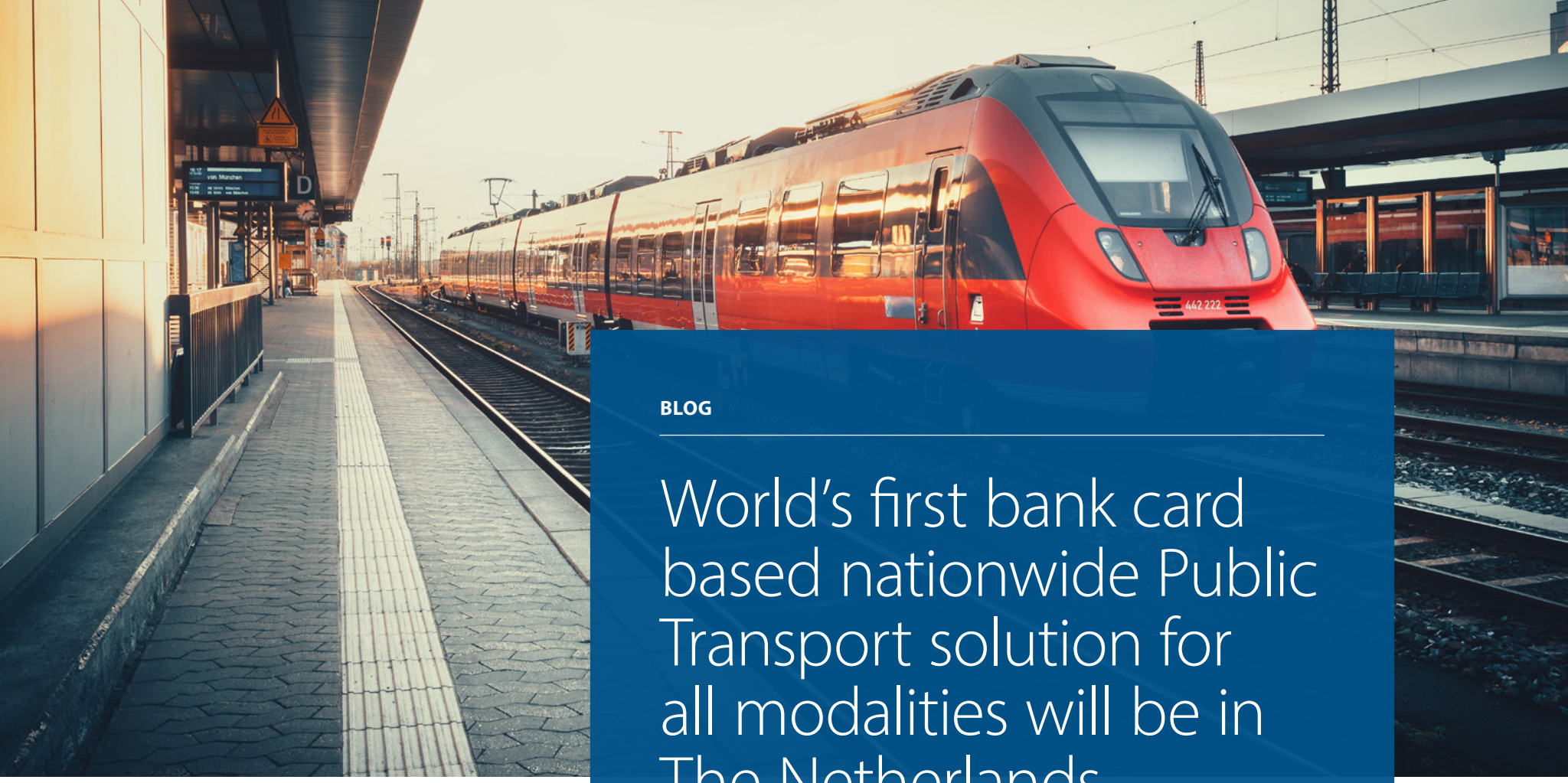
Let's make history

Cast your mind back to the early days of the internet, just before standards such as TCP/IP were agreed. All that is history now, but we have reached a similarly pivotal point today. We need to create a European soft infrastructure for data sharing based on a sound consent mechanism which works for every person, business and government. So I call on you to join me in shaping the future. Let's make history again!

Author
Mariane ter Veen

ORIGINAL BLOG

GET IN TOUCH



BLOG

World's first bank card based nationwide Public Transport solution for all modalities will be in The Netherlands

26 November 2019

Pepijn Groen

Jorrit Penninga

GET IN TOUCH

INNOPAY

Our involvement in the launch of the Europay Mastercard Visa contactless (EMVc) card was a great reminder of the benefits of a shared perspective. EMVc has already been rolled out in public transport in various geographical regions (e.g. in London, New York, Singapore, Sydney & Chicago), but nowhere nationwide and all modalities. It gives passengers instant mobile access to transit and eliminates the need to queue for ticket machines. Providing people with the convenience to travel seamlessly with multiple operators requires nationwide adoption and interoperability. To make this happen, card issuers and public transport operators (PTOs) have engaged in a unique cross-sectoral collaboration. For such an initiative to be a success, it is crucial that all parties put their own interests aside and collaborate from a shared perspective right from the start. The common aim should be to envision and realise opportunities for synergy. In the case of EMVc, this is what is enabling both the payments industry and the transport industry to seize opportunities for transactional growth in the mobility ecosystem.

Transactional growth for everyone

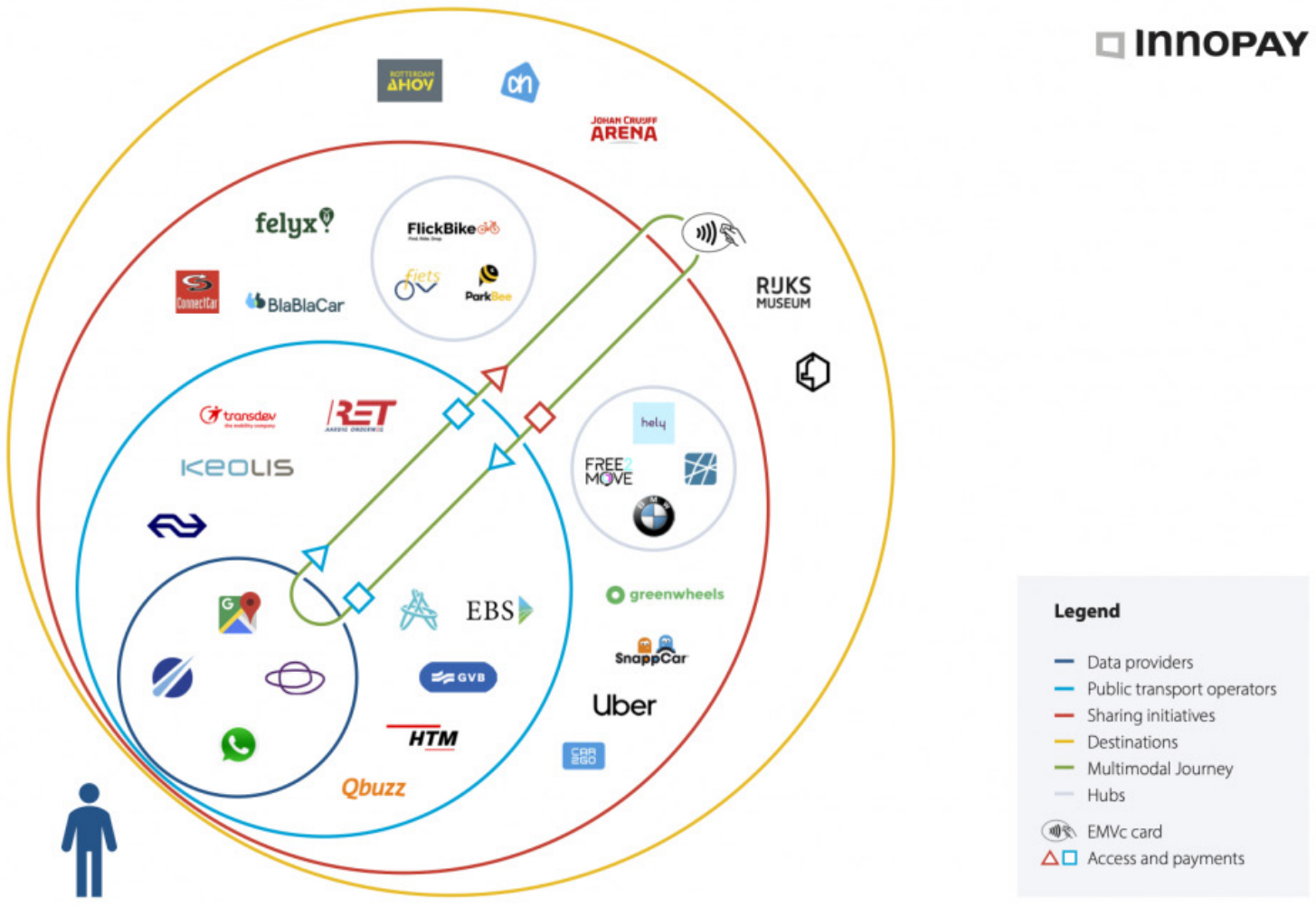
In the collaborative partnership for EMVc, the PTOs and card issuers had a clear shared interest: transactional growth (i.e. completed journeys for the PTOs and card transactions for the issuers). Furthermore, for PTOs, a 'dual-market' payments platform opens up various new travel methods such as sharing services. Passengers can tap in and out between different operators using the card itself, their smartphone or wearables. In addition, EMVc has security mechanisms to cover various risks and

liabilities associated with interoperability between operators. For card issuers, meanwhile, the project is an opportunity to increase their relevance to their customers and to extend contactless payments from the retail sector into the mobility context – including PTOs and car and bike-sharing services.

Leverage trust instead of competing on trust

So how could that be achieved? To realise the potential for transactional growth, we advised the card issuers and PTOs to set up a trust framework that builds upon the EMV® specifications. A trust framework or scheme consists of additional agreements on business, legal, operational and technical aspects. These agreements establish the shared interests and the required level of trust between organisations such as operators, service providers and others to facilitate transactions through the platform. The agreements cover matters such as governance, additional risks, additional liabilities, security, service availability and admission of new user groups. The trust framework is designed to attract as many user groups to the platform as possible.

Meanwhile, passengers enjoy an optimal payment experience throughout their journeys. They can link their EMVc card to a mobility account and unlock access to a wide array of services in the mobility ecosystem, varying from Netflix-inspired 'Mobility as a Service' (MaaS) subscriptions to regular public transport access. Figure 1 visualises the footprint of an EMVc-based payments platform in the ecosystem and how the EMVc card is used to access and pay for mobility services throughout the multimodal journey.



More growth opportunities based on synergy benefits

Such a trust framework also enables card issuers and public transport operators to further leverage their collaboration in the mobility arena to realise pioneering growth beyond payments alone. The underlying trend is the shift from asset-based to usage-based mobility, which will increase the number of mobility providers in the ecosystem. This will result in more opportunities to capture value, such as by expanding in the ecosystem and making a positive socio-economic impact. We see particular opportunities for synergy benefits in the following three areas:

1. Data sharing

Customer-centric data sharing is the foundation of future-proof mobility. Data sharing between providers enables more accurate journey planning, easy onboarding across apps, and journeys based on passengers' actual preferences. All this contributes to a seamless customer experience. The trust framework initiated by this collaborative partnership could evolve into a trust framework for data sharing between all providers in the mobility ecosystem.

2. Geographical diversification

Further developing the interoperability between providers to expand into surrounding geographical areas is an opportunity to create transaction growth for PTOs while offering a more seamless customer experience on longer-distance journeys.

3. Mobility solutions

The card industry and PTOs can leverage their resources to develop joint mobility solutions for shared growth. An example of such an initiative is 'KBC Olympus', a MaaS proposition for enterprises developed by KBC Bank and Belgian public transport companies, aimed at better distributing mobility demand and reducing congestion.

INNOPAY is involved as a strategic partner in the Dutch 'Innovation in Payments' project, within which PTOs and card issuers are collaborating to implement EMVc. Please contact us if you would like to learn more about this initiative or to discuss how we could help you.

Authors

Pepijn Groen and Jorrit Penninga

ORIGINAL BLOG

GET IN TOUCH

BLOG

7 Steps Towards Giving Your Customers Control over their Data

27 December 2019

Mariane ter Veen

Every minute, on a global level, people send 156 million emails, conduct over 3.5 million searches in Google, and order over US$250,000 worth of goods from Amazon. These are staggering numbers, and the exchange of data is set to continue to grow exponentially.

Smart organisations realise the potential of this data and are continually looking for ways to create value. At the same time, consumers are becoming increasingly aware of their central role in all this; after all, it's their data, isn't it? So shouldn't the 'data benefit balance' tip in their direction?

There are several reasons why 'data sovereignty' – control over data – should be the central design principle of not only the data economy as a whole, but also of every organisation's own data architecture. Giving people control over their data and offering fair value in return is an effective way for organisations to improve their customer relationships. Consumers are more willing to share data with organisations they trust, and more trust means a lower transaction cost for data sharing. This results in better access to the data needed to build and grow a business and opens up new opportunities for creating value for customers.

So in order for both businesses and consumers to truly thrive on all the benefits of data sharing, organisations should start tackling the data sovereignty challenge today. But how? Here are seven ways to give your customers control over their data:

GET IN TOUCH

INNOPAY

Figure 1: 7 Steps Towards Giving Your Customers Control over their Data

1. Create awareness internally

In most organisations there is little awareness about data sharing – neither in terms of the importance of data sovereignty for customers, nor the possible business potential. Communicate your vision and strategy clearly internally, and ensure everyone embraces it. The sovereignty of customers' data should be kept in mind in all processes. Truly tipping the data benefit balance in the customer's direction also means exploring the potential of using data to create new products and services that benefit customers. Remember: customers are willing to pay for added value.

2. Evaluate your internal capabilities

Does your workforce have the right knowledge and experience of data sharing? Do you need to create and fill new roles (partner network managers, data managers and so on)? What is the best way to secure the right talent (by recruiting to your own payroll or by working with a flexible workforce for maximum agility)? Which profiles will you need in the next five to ten years?

3. Optimise your own systems and processes

Re-assess your own systems and processes. Can you separate the data from the processes and reuse data internally? And don't forget to optimise data-heavy processes, such as your customer onboarding process; it should be seamless to ensure that they immediately recognise your digitally responsible attitude towards using their data. Needless to say, it is essential to constantly protect your systems and database against intrusion and data leaks, and for your customers to have the peace of mind that their data is safe in your hands.

4. Create alignment

You are part of a data-sharing chain – not only receiving data from your customers, but also providing data to your suppliers and other business partners. Ensure that they offer you the same transparency that you provide to your customers. Ideally, you should take a proactive approach to creating alignment throughout the chain. Use the INNOPAY 9 building blocks model to align legal, technical, business and governance considerations.

5. Review your role in the ecosystem

Analyse not only your need-to-have data but also the 'nice-to-have' data – the data that will help you to create more value for your customers so that they feel more rewarded for sharing their data with you (and hence will ultimately share even more). Can you obtain that from partners in your current ecosystem, or do you need to expand your ecosystem by adding new partners? And what does this mean for your role in this ecosystem?

6. Provide a user interfacE

Offer your customers a user interface or control panel to allow them to manage which data they are willing to share with you and when. This will establish the necessary foundation of trust for data sharing and – perhaps surprisingly – tends to lead to your customers providing more data rather than less.

7. Communicate transparently

Big data comes with a big responsibility to be transparent about the information you gather. This might sound obvious, but most organisations are not really transparent about what data they collect and why. Be open with your customers about the data you require from them. Demonstrating that they receive a fair value in return will earn you their lasting trust and will ultimately encourage them to share even more data with you.

These seven steps will help you to consider many key aspects of the data-sharing process to continuously strengthen your relationships with customers. As they discover the rewards of sharing data with trusted partners such as yourself, they will become increasingly willing to share more information… which you can then leverage to truly thrive as we move into the digital transactions era.

At INNOPAY, we have already helped numerous customers to speed up their business based on the existing standards, regulations and data-sharing schemes. To tap into our experience and benefit from our proven approaches, or if you have any questions or would like more information, feel free to contact us.

Author
Mariane ter Veen

ORIGINAL BLOG

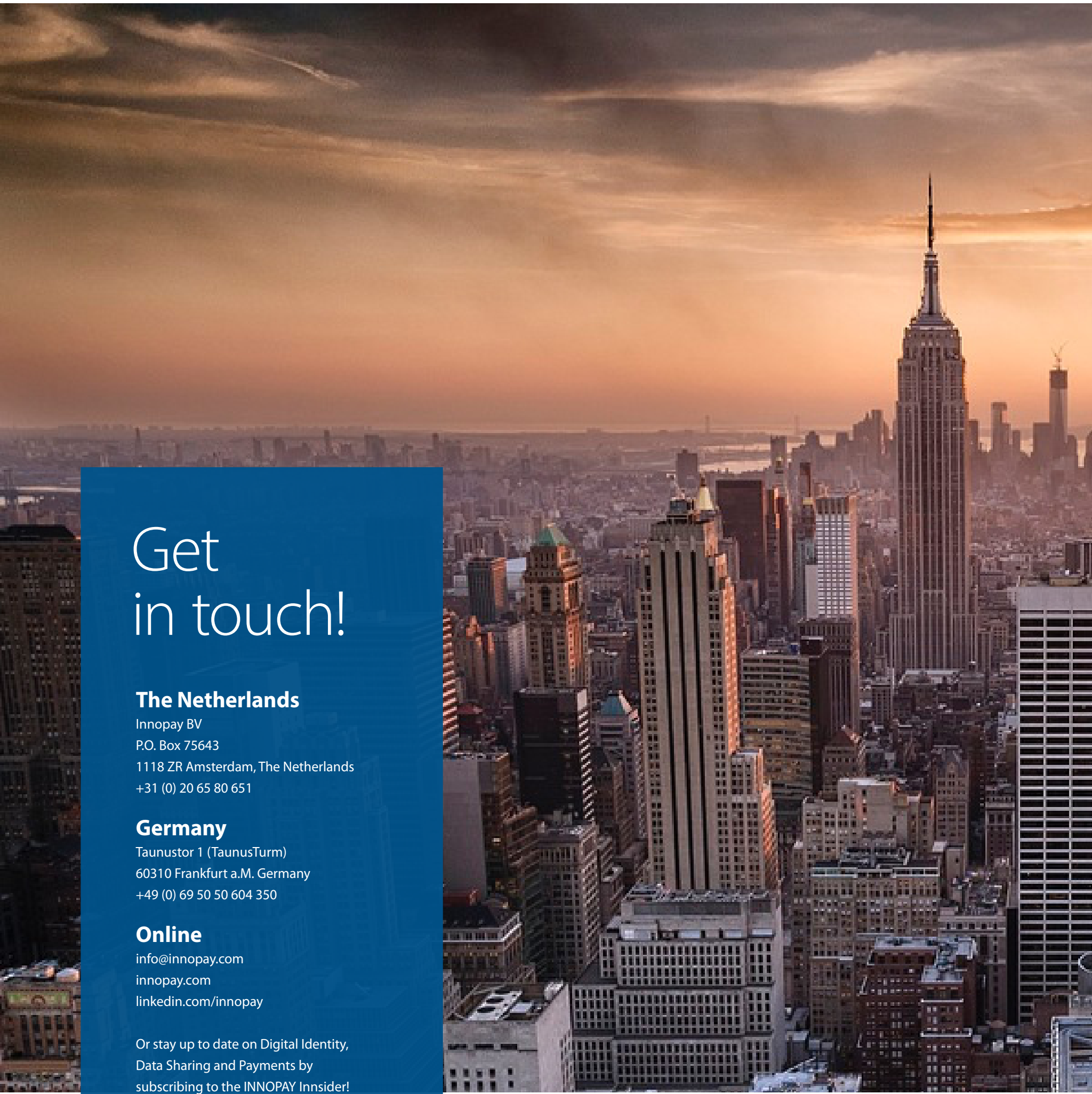
GET IN TOUCH

Everything Transaction

About data, trust and the massive opportunities of the transactional Internet

Dutch **Management Book of the Year** 2019

INNOPAY



Get in touch!

The Netherlands

Innopay BV
P.O. Box 75643
1118 ZR Amsterdam, The Netherlands
+31 (0) 20 65 80 651

Germany

Taunustor 1 (TaunusTurm)
60310 Frankfurt a.M. Germany
+49 (0) 69 50 50 604 350

Online

info@innopay.com
innopay.com
linkedin.com/innopay

Or stay up to date on Digital Identity, Data Sharing and Payments by subscribing to the INNOPAY Innsider!