



Book  
of Insights  
2019

EVERYTHING TRANSACTION



# Table of Content

<b>Foreword</b>	<b>3</b>
<b>Trust Framework in Practise</b>	
iSHARE data sharing scheme now available for everyone in the logistics sector	5
Integrating different modalities and services into an open mobility ecosystem: five key steps	7
Collaborative data sharing drives digital transformation	10
<b>Innovation in banking</b>	
Digital consent management is key for data opportunities	12
Corporate customers are pivotal in creating value on top of Instant Payments infrastructure	15
<b>Cybersecurity &amp; Privacy</b>	
Decentralised identity enabled by the data control stack turns GDPR into a competitive advantage	18
Customer data: old problems demand new solutions	21
Looking for the missing part of GDPR: a 'soft infrastructure' for sharing your data	23
Quantum computers will revolutionize cryptography and cybersecurity. Here's why.	26
<b>PSD2 &amp; Open Banking</b>	
Mastering Open Banking: How the 'Masters in Openness' create value	29
Sharing transaction risk data leads to Open Banking success	41
Seamless, Uber-like payments, brought to your bank account	45
<b>Open Insurance</b>	
Insurance and the Open Banking wave: seven use cases	47
'Open Insurance': a new mindset for the Insurance sector	50
How #openness will change insurers' pricing strategies	52
Note to Insurers: silence does NOT imply consent	55
<b>Onboarding in Financial Sector</b>	
A pragmatic guide to embracing innovative CDD technologies	58
The battle is ON: incumbent banks accelerate onboarding innovations	62
How banks can solve the "Onboarding Puzzle" in the German market	66
Open Banking and TPPs trigger banks to innovate their corporate onboarding processes	71
<b>Get in touch!</b>	<b>74</b>





# Foreword



**Shikko Nijland**  
CEO and  
Managing Partner

**GET IN TOUCH**

**Interactions and transactions are like breathing. We do it all day, usually without problems, and we don't really think about it. When we send someone a message, buy something in a store, book an airline ticket online or conclude a professional deal, but also when we log onto a platform like Twitter.**

**The Internet can be seen as the dynamic underlying infrastructure for interactions and transactions between all kinds of parties, both people and organizations. It is an infrastructure that is under continuous development. Within a few decades, the Internet developed from an information channel into an interactive medium, that is gradually being made suitable for transactions. Each stage of the web has its own dynamics. By now, most people understand the enormous impact digitization has on all kinds of markets, and with that on our daily lives.**

**However, we have found that the combination of the two subjects of 'transaction' and 'Internet' to date has received relatively little attention. Taking a look at the Internet and digitization from the perspective of transactions brings a lot of things together.**

## **Digital trust**

The core concept from where 'Internet' and 'transactions' come together is the word 'trust'. Trust is what drives transactions and it manifests itself in the digital domain in a completely different way from what we are used to in the physical world, namely in the form of data. While, on the one hand, personal information is needed to complete a

digital transaction, to gain the trust of the people involved, on the other hand, people have become more suspicious when it comes to the way that information is being handled. Scandals about data leaks, election rigging, privacy concerns, the inability of platforms like Facebook to process enormous amounts of data in a secure way: they are all expressions of those same concerns.

### **The transactional Internet**

In the meantime, organizations are working on platforms and ongoing digitization, but at the same time, they systematically underestimate them. As a result, they make decisions that often optimize the existing situation, but that are insufficient to provide a genuine solution to the more fundamental problem of trust, which is only possible by working together on an entirely new transaction infrastructure with new business models, the 'transactional Internet'. Trust will to a far lesser extent be provided by institutes, like businesses and governments, but will be embedded in the infrastructure on the basis of mathematical formulas and cosmic laws. A shift from institutional towards infrastructural trust.

The emergence of distributed computing and blockchain technology, with implementations like Bitcoin and Ethereum, indicates that it is possible to organize trust differently and carry out transactions without far-reaching intervention from platforms. There is still a lot of work to do, but the technology is there.

### **The two big fixes**

There are basically only two things that need to be solved to make that next phase possible. Two 'big fixes' to generate digital self-determination and with it a stronger foundation for the inevitable further digitization and ongoing platformation.

First of all, we need to solve the trust paradox, which refers to the opposite needs on the part of users to make their data, in particular their personal data, more open and at the same time secure it more effectively, to maintain their trust in further digitization. That can be done by giving back consumers control of 'their' data, after which they can consent to share elements of their data with third parties.

The second big fix is to restore the so-called data benefit balance, so that not only organizations and platforms benefit from the revenues generated from data, but consumers as well. The benefits for consumers of the transaction data they help generate are very small compared to those of their professional counterparts. Balance can be restored by allowing consumers to share in the revenues of their data.

### **Opportunity, action!**

When the two big fixes have been carried out, the transactional Internet has arrived. We are not there yet, but we have a tremendous opportunity to change the digital playing field on a global scale.

INNOPAY is committed to helping our clients to move forwards with all these challenges by working with them to capitalise on the huge opportunities offered in this ever-changing environment.

We do this by being different. By innovating and not being constrained by conventional thoughts. By approaching everything from our clients' perspective – understanding their ambitions and working side-by-side to meet them. In our new book "[Everything transaction](#)" you can read more about our vision on these challenges and possible solutions.

In this book, our Book of Insights, you can find a selection of our consultants' evaluations and predictions on Data sharing, Openness, Customer in Control and Digital Transformation.

We trust these insights will help to bring you continued success in 2019.

Shikko Nijland

**Author**

Shikko Nijland

[BACK TO INDEX](#)

[SUBSCRIBE FOR  
NEWSLETTER](#)





## TRUST FRAMEWORK IN PRACTISE

# iSHARE data sharing scheme now available for everyone in the logistics sector

Eefje van der Harst on April 3<sup>rd</sup> 2018



**Eefje van der Harst**  
Manager

[GET IN TOUCH](#)

**INNOPAY is proud to announce that as of March 2018, all organisations active in the logistics sector can make use of iSHARE. This scheme, or uniform set of agreements, which enables everyone in the sector to share logistics data with everyone else – including with partners further upstream or downstream in the chain – in a simple and controlled way, was launched during the annual conference of the Dutch Top Sector Logistics. The launching customers were also presented to the audience at the event.**

iSHARE is a scheme, or set of agreements, that enables safe data sharing across the logistics sector. The scheme includes Functional, Technical, Legal and Operational agreements, co-created by the sector itself. iSHARE's goal is to significantly lower barriers to new data sharing relationships between all parties adhering to the agreements. By agreeing to use the same technical standards to identify, authenticate and authorise each other, and by agreeing to only use shared data for the purposes specified under iSHARE, adhering parties reduce the time spent to integrate software solutions and to get to know and trust each other.

Throughout 2017, more than 20 logistics parties – public and private, large and small, and active in various modalities – contributed to working groups which co-created the iSHARE scheme. These working groups, and the co-creation process in general, were chaired and facilitated by INNOPAY. The set of agreements was tested and proven through

a series of Proof of Concepts, such as the one presented by Ritra Cargo, Yellowstar and Portbase in a [webinar](#) earlier this month. iSHARE was officially launched during the annual conference of the Dutch Top Sector Logistics, and **12 selected companies** will start to implement the scheme in H1 2018.

### **INNOPAY and scheme development**

INNOPAY has a rich history of being involved in the development of schemes including iDEAL, eHerkenning, Simplerinvoicing and others. The key to success is our inclusive style of development. By inviting parties to co-create schemes **for the market** and **by the market**, we ensure that agreements are highly relevant and supported by the sector. INNOPAY's knowledge and expertise of Functional, Technical, Legal and Operational domains ensures that agreements represent a balanced representation of stakeholder needs.

### **'Everything Transaction'**

Schemes such as iSHARE fit perfectly with INNOPAY's vision on data sharing. As data becomes more valuable, we strongly believe that all data sharing is becoming a series of transactions based on the exchange of value. This means that INNOPAY's digital transaction expertise is now highly relevant across many domains and sectors, including logistics.

INNOPAY believes that access to data, rather than the data itself, should be centralised. If parties agree on standardised ways to provide each other access to data – specifically on how to identify, authenticate and authorise each other – the data can remain at the source with no need to store them in (additional) platforms. This negates the need for additional software

solutions, and prevents further fragmentation. The shared way of accessing data allows all parties to continue providing data services through their preferred technology solutions, to create business value as they see fit, to increase service reach and conversion, and to minimise costs.

### **iSHARE's ambitions**

INNOPAY will continue to facilitate iSHARE's adoption before transferring the management of the scheme to an independent scheme owner, as we did to the **Dutch Payments Association** for iDEAL and to **Logius** for eHerkenning. Meanwhile, INNOPAY also facilitates the international adoption of iSHARE.

If you are a logistics organisation interested in sharing data in a uniform, simple and controlled way, please visit [www.ishareworks.org](http://www.ishareworks.org).

If you found yourself in a fragmented market with high barriers to sharing data, a scheme like iSHARE might be exactly what is needed. Please contact iSHARE project manager Mariane ter Veen for more information on how INNOPAY can help you.

**Author**

Eefje van der Harst

[ORIGINAL BLOG](#)

[BACK TO INDEX](#)

[SUBSCRIBE FOR  
NEWSLETTER](#)





TRUST FRAMEWORK IN PRACTISE

# Integrating different modalities and services into an open mobility ecosystem: five key steps

Pepijn Groen, Tjerk van Dalen on August 6<sup>th</sup> 2018



**Pepijn Groen**  
Senior Consultant

[GET IN TOUCH](#)



**Tjerk van Dalen**  
Consultant

[GET IN TOUCH](#)

**Public transport organisations and mobility sharing initiatives all share the same ambition: getting commuters out of their private cars. How? Make end-to-end commuting as convenient as car ownership, but for less money. In practice, mobility providers can't individually satisfy these criteria since they have limited reach and availability. Providers should collaborate in ecosystems to incorporate their services with those of others and develop (better) multimodal mobility propositions. This blog provides a view on open mobility ecosystem and five key steps to organise it.**

## **Open mobility ecosystems facilitate better travel propositions**

Technology developments (e.g. APIs), regulatory changes (e.g. PSD2, GDPR) and collaborative mindsets enable digital collaboration between players in value chains. These collaborations aim to develop new business models, to innovate services and to decrease inefficiencies. Ultimately these collaborations grow into digital ecosystems. APIs play an instrumental role in ecosystems by sharing business data, functionality and user experience in a controlled fashion. First sparks of digital ecosystems are visible in the energy, agriculture and logistics industry (e.g. JoinData, NEDU, iSHARE).

Mobility would be an obvious industry to apply such an ecosystem. A digital ecosystem for mobility should integrate the services of Public Transport Operators (PTO), data providers, sharing initiatives, techs and other parties that take part in multimodal travel. For example, PTOs and sharing initiatives can integrate existing propositions to improve

interoperability and provide more personalised travel options. Whereas data providers can help find solutions to better utilise vehicle capacity. A visual representation of an open mobility ecosystem is provided below where similar providers are categorised in a layer.

The more ecosystem players work together, the more convenience in multimodal travel propositions can be achieved. For example, integration of public transport and other mobility providers could result in Mobility as a Service (MaaS) propositions (e.g. [Whim](#)). Extending MaaS with destinations further optimises journeys for customers and provide opportunities for new service offerings (i.e. Hospitality as a Service).

### 'Customer in control' is a key driver for ecosystems

In multimodal travel, it is essential to allow customers to onboard and plan their journey as quickly and as easy as possible, to compete with car ownership. INNOPAY strongly believes that an open mobility ecosystem provides the most value when customers are in control. Customers should be able to access services quickly and trigger data exchanges between ecosystem players (e.g. account information, travel preferences, travel and transaction history) to generate optimal travel options at all times. This should be done based on a verified identity of the customer and a form of 'digital consent management' <sup>1</sup>. Digital consent management allows customers to control who can access what personal data and specify these access rights, preferably in a centralised dashboard. This allows customers to determine from what ecosystem players they would like to receive offerings or integrate services.

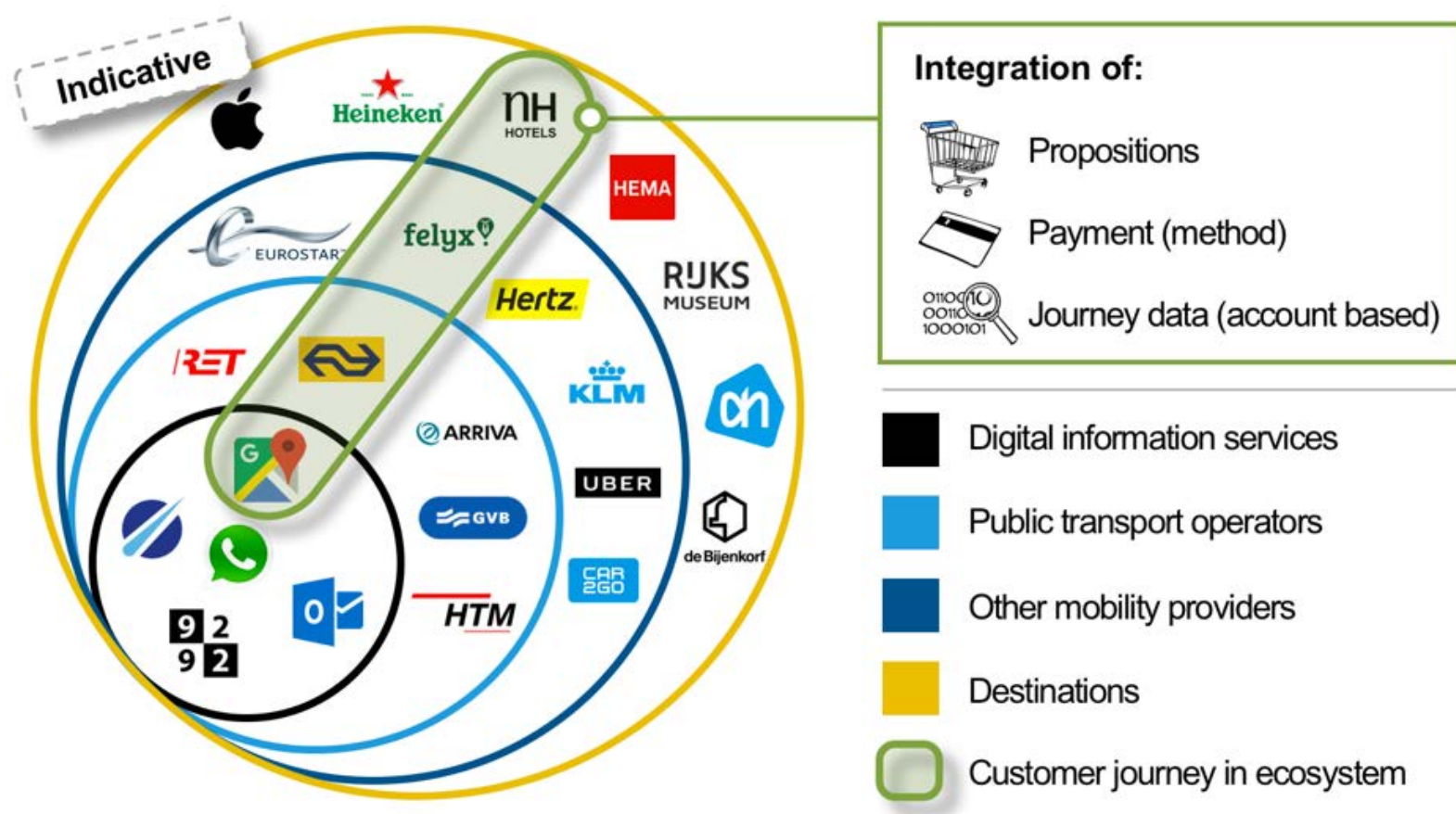


Figure 1.



## Five essential bridging steps towards open mobility ecosystem

Mobility providers are already collaborating to improve multimodal travel on themes such as payments (e.g. Dutch OV-chipkaart) and journey planning (e.g. Google Maps, CityMapper, Waze, Here WeGo). These existing collaborations could serve as foundation for an open mobility ecosystem. Based on INNOPAY's experience five essential steps are provided to further explore the implementation of an open ecosystem:

1. **Identify use cases.** Identify relevant use cases of integrated customer journeys with real added value for customers and all players involved
2. **Shape coalition of the willing.** Shape an initial coalition of the willing around each use case to operationalise these use cases
3. **Form ecosystem agreements.** Create a set of agreements

that help players to take position in the mobility ecosystem and participate. Agreements could include:

1. Design principles
  2. Roles and capabilities
  3. Required tools and standards to share data and manage consent
  4. Governance (if desired)
  5. Legal framework (if desired)
4. **Pursue growth.** Adding participants and layers to the ecosystem will increase user base and increase added value of use cases.
  5. **Diversify.** After a few successful use cases, ecosystem participants can further explore future opportunities.

Are you a mobility provider who is interested in further exploring opportunities of an open mobility ecosystem? Please contact the authors.

1. Source: <https://innopay.com/blog/customer-data-old-problems-demand-new-solution...>



### Authors

Pepijn Groen, Tjerk van Dalen

ORIGINAL BLOG

BACK TO INDEX

SUBSCRIBE FOR  
NEWSLETTER



TRUST FRAMEWORK IN PRACTISE

# Collaborative data sharing drives digital transformation

Mariane ter Veen on November 6<sup>th</sup> 2018



**Mariane ter Veen**  
Director, Lead Data  
Sharing

[GET IN TOUCH](#)

**Open and collaborative exchange of data between organisations, their partners, customers and competitors is increasingly being powered by trusted data sharing networks. And as with every paradigm shift, this new reality heralds both opportunities and risks for players in all sectors.**

## Data sharing in a world where Everything's Transaction

"What really excites me about this new role is the opportunity to support our customers with a challenge which is here right now," enthuses Mariane, who has a wealth of experience in this domain. Before spearheading the development of our logistics data sharing scheme – iSHARE – she led a number of high-profile data exchange initiatives across different industries.

"Data sharing is in INNOPAY's DNA," continues Mariane. "We see a world where trusted data exchange is the key to unlocking new business models and reducing costs. Companies are presented with a choice about how they see their future. They can evolve, adopt a more open outlook, collaborate across their ecosystems, and maximise new opportunities. Or they can remain siloed, reject opportunities to share data in trusted environments, and gradually calcify into irrelevance. The regulated financial world with e.g. payments and securities is an early manifestation of this ecosystems thinking. We believe that digitisation will drive much more of this or we'll end up in a fragmented services world. For transaction services this is not practical and holds back the potential of the digital economy.



“We believe our customers are ready to embrace a new way of doing business. My role is to help them articulate their data sharing vision, and guide them through the journey.”

### **Working together is the way forward**

A common response to the data sharing challenge has been the platform-based approach; organisations develop their own proprietary platforms or engage in bilateral agreements with key suppliers or partners. This approach can be expensive, time-consuming, difficult to scale, and ultimately leads to data isolation. Mariane proposes a fundamentally different solution.

“In a world where everything’s transaction, companies need to play a more active and inclusive role in their data ecosystems. We serve our customers by helping them achieve the required level of openness whilst always ensuring that their own customers remain in control of their data. Real business opportunities come from working together, even with competitors and previously unknown parties.

### **Trust is the key to unlock data sharing opportunities**

Mariane believes that “trust” is the essential ingredient to ensure effective data sharing. “Trust will be the driver for collaborative data sharing. In our view, the creation of a scheme or trust framework will enable our customers to exchange data more easily, and reap their own specific benefits and competitive value from within the broader ecosystem.

There is a real space in the market for soft infrastructures; sets of agreements enabling data sharing. These will create a more equitable power balance between users and platform owners in both the control of data, and also in the value which can be realised from that data.”

Organisations are presented with both opportunities and risks by the transition to trusted data sharing. New and innovative business models will be enabled by a greater capacity to drill into extended data sets shared with suppliers, partners and even competitors. Increased trust will also deliver cost efficiencies by lowering transaction management costs.

If trust is established between parties, it will be easier, faster and cheaper to do business together. Outlays on technical infrastructures and legal agreements will be lowered. On the reverse side, failure to act now could leave companies increasingly out in the cold.

### **iSHARE is a scheme which will facilitate openness across multiple sectors**

iSHARE is a tangible example of INNOPAY’s ability to support customers in making this transition. It is a set of agreements which enables players across the logistics industry to share data with each other on the basis of mutual trust; irrespective of type, size, modality and jurisdiction. It is not a technology solution, instead the shared agreements provide all the essential functional, technical, legal and operational standards that are needed for organisations within the iSHARE community to share data.

Mariane sees iSHARE as a template which will be used to unlock effective data sharing across a wide variety of industries. And INNOPAY is uniquely qualified to help organisations to sidestep the challenges of developing this type of collaborative soft infrastructure.

“We’ve dealt with many challenges such as the involvement of a wide variety of stakeholders with their own specific interests. When we facilitate projects like iSHARE, we focus on very tangible goals and objectives, and agree what needs to be delivered to unlock business value for each stakeholder. We listen carefully to their objectives, and take them on a journey which reveals common interests across the community as well as their own local aims. This is how we make data sharing schemes like iSHARE successful. It’s a model we want to deploy to help new customers.”

### **Now is the right time to get ahead of the game**

“The opportunity is here now,” concludes Mariane. “If you don’t act, someone else will. This is all about your future position in your value chain. And whether you take this opportunity to improve your business for both yourself and your customers by sharing data more effectively.”

**Author**

Mariane ter Veen

[ORIGINAL BLOG](#)

[BACK TO INDEX](#)

[SUBSCRIBE FOR  
NEWSLETTER](#)



## INNOVATION IN BANKING

# Digital consent management is key for data opportunities

Mounaim Cortet, Douwe Lycklama  
on June 29<sup>th</sup> 2018



**Mounaim Cortet**  
Senior Manager and  
Lead Strategy

GET IN TOUCH



**Douwe Lycklama**  
Founding Partner

GET IN TOUCH

During the last EBA Day (12 June), the Euro Banking Association published their thought leadership paper “B2B data sharing: digital consent management as a driver of data opportunities”. This paper is a joint effort of INNOPAY and the EBA’s Open Banking Working Group. Below you will find the executive summary of the paper, you can find the full paper [here](#).

A short summary of the paper can be found on the following pages:

Data sharing can help to increase efficiencies, lower risks and contribute to service innovation. Over the past two decades, digitisation has not only increased the amount of existing data but also increased the sharing of data between individuals and businesses. However, multilateral (‘many-to-many’) relations in data sharing between businesses and their service providers, including banks, have not yet become widely established. Instead, a scattered landscape of business-to-business (B2B) exchange platforms, actors and bilateral projects has evolved.



The rise of B2B exchange platforms has led to business data accumulation by third parties, who use these data for analytics and value creation. For banks, the strategic implications include:

- Limited overview and insight into data about the end-to-end trade process, impacting the understanding of customer needs;
- Sharing of 'added value' with platform service providers that will leverage data capabilities to offer business customers new propositions;
- Risk of client disintermediation as platforms increasingly build seamless and comprehensive digital experiences, satisfying both financial and non-financial needs of corporate customers.

Meeting these challenges requires improvements in data accessibility, ensuring a free flow of data, enabling market actors including banks to access business data more easily, within businesses directly or indirectly via B2B exchange platforms.

'Digital consent management' lies at the heart of any possible solution for the challenges ahead. Digital consent is obtained from businesses, mandating banks (and/or other service providers) to obtain and use business data to innovate their services for the benefit of businesses. This concept is similar to the provisions of the revised Payment Services Directive (PSD2) and the General Data Protection Regulation (GDPR), which aim to improve customers' control over their data through the right to provide (or withdraw) consent to allow authorised third parties to access their personal and business information in order to use their services.

Banks traditionally play a role in the value exchange because of their trusted and regulated position. As data exchange is increasingly fraught with operational complexity and liabilities, banks can leverage this trust to play a crucial role in such consent transactions, thereby improving their access to business data (see figure 1).

Improved access to data allows banks to:

- Improve the efficiency of financing and risk processes contributing to the financial bottom line;
- Reduce cost to serve un- or under-addressed business segments, e.g. long tail of SMEs, opening up additional markets;
- Pursue data-driven propositions as part of an open banking strategy to strengthen the relationship with business clients.

For business clients, such improved access to data means a higher benefit of their data beyond the bespoke platform applications where the data is currently held. For B2B platforms, it means answering to customer demand to be in control of their data, potential regulatory pressure focused on ensuring free flow of B2B data, while also creating the opportunity to commercially leverage their position as the data holder.

To foster a wide adoption, data sharing needs to be standardised to enable businesses, B2B platforms and banks to seamlessly exchange data in a many-to-many relation. Standardisation of digital consent is also expected to reduce the transaction costs of data exchange. Figure 2 provides an overview of such consent relations and data sharing. In this example the buyer is the business providing consent to the bank, but this could also be the seller.

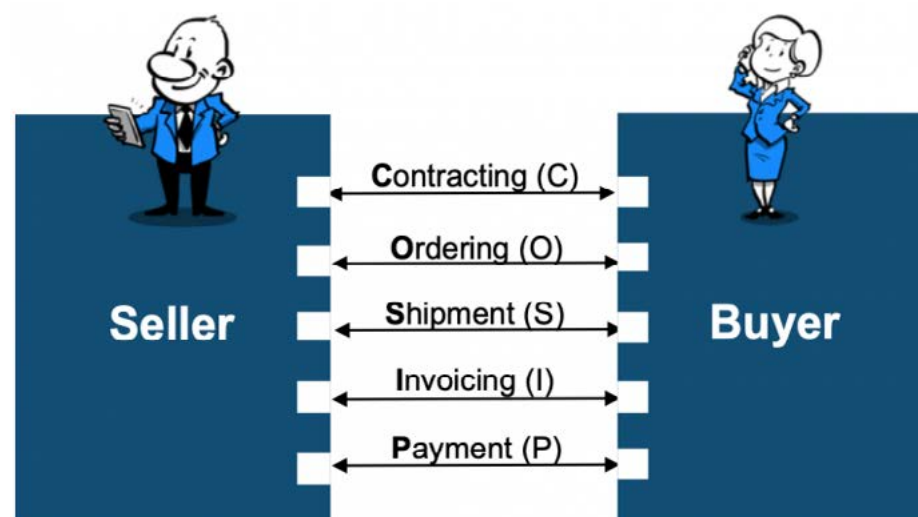


Figure 1.

By actively pursuing improved B2B data accessibility, banks have an opportunity to revise their digital agenda for corporate and SMEs through:

- Creating awareness among business clients regarding the potential benefits and new value propositions emerging from improved access to data;
- Addressing potential changes to operating models (customer relationships, products and management) and business models enabling new value propositions;
- Considering options for industry collaboration to drive ubiquitous adoption of standardised consent management and data sharing.

The full paper “B2B data sharing: digital consent management as a driver of data opportunities” can be found at the [website](#).

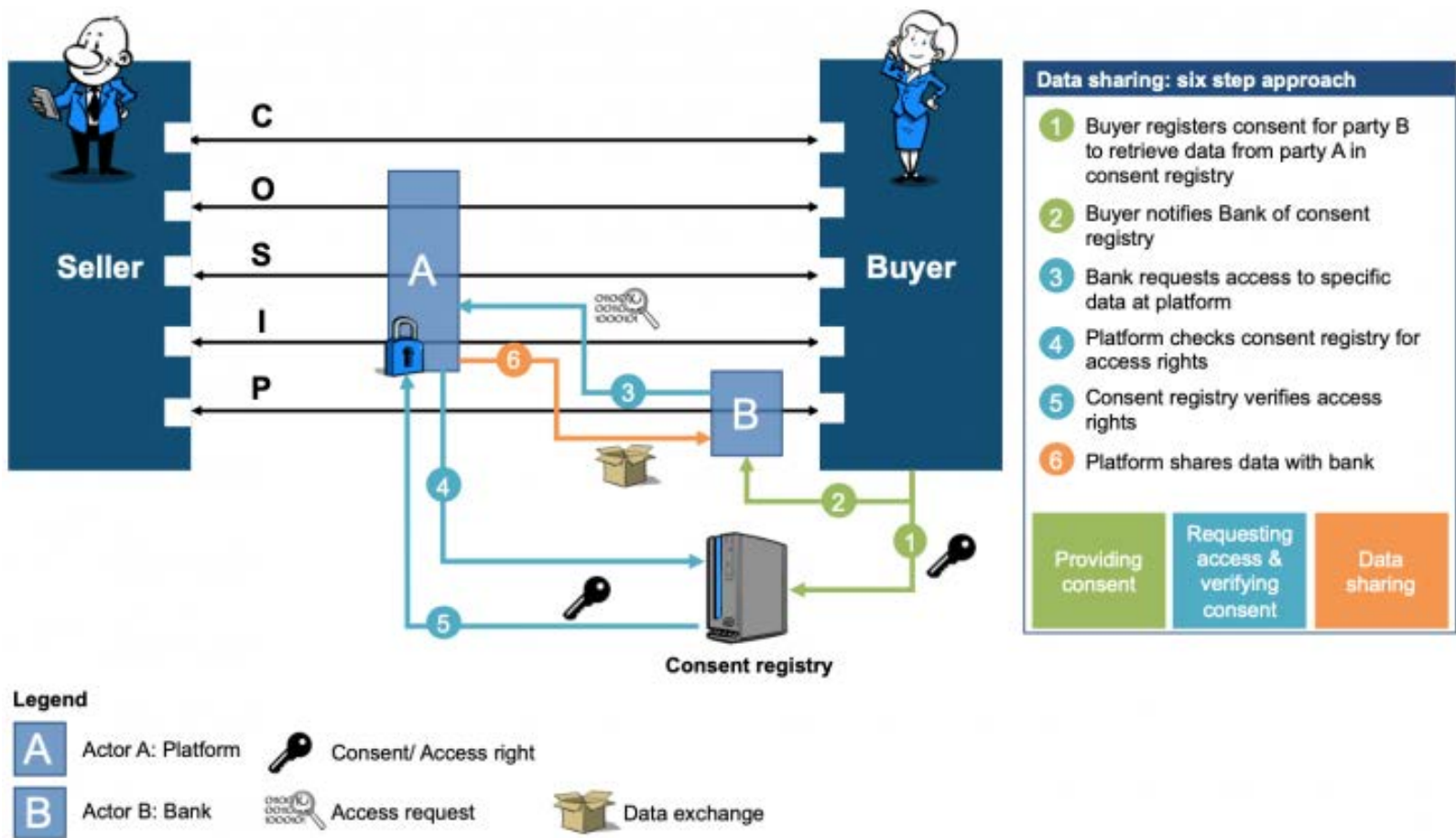


Figure 2.

## Authors

Mounaim Cortet, Douwe Lycklama

[ORIGINAL BLOG](#)

[BACK TO INDEX](#)

[SUBSCRIBE FOR NEWSLETTER](#)



# Corporate customers are pivotal in creating value on top of Instant Payments infrastructure

Leon Koesoemowidjojo, Wouter van den Hengel  
on August 7<sup>th</sup> 2018



**Leon**  
**Koesoemowidjojo**  
Senior Consultant

[GET IN TOUCH](#)



**Wouter**  
**van den Hengel**  
Consultant

[GET IN TOUCH](#)

**As Instant Payments is expected to become the new normal in payments in many countries, it is imperative for financial service providers to offer Instant Payments capabilities to remain relevant in the future. The significant investments required to update current payment infrastructures motivates financial service providers to look for relevant use cases and create value-added services for their customers.**

In this blog, we explain why financial service providers should aim Instant Payments value-added services towards corporate customers rather than retail customers.

## **No profitable use cases for retail customers**

Instant Payments (IP) use cases may be found for both retail and corporate customers. However, offering relevant IP use cases for retail customers, appears to be quite challenging, mainly for three reasons.

### **1. Keep up, customers already expect instant services**

Today's retail customers expect digital services that are always online, instantly available and on-demand. We live in an online society, where we can communicate with each other through a variety of social media possibilities instantly. Examples that have shaped consumer expectations are media streaming services such as Netflix, online shopping platforms like Amazon and (challenger) banks enabling customers to open an account in a matter of minutes at any time.



Figure 1.

Retail customers simply expect financial service providers to deliver a similar level of service for payments. Offering anything less than IP is a dissatisfier for them and opens the door to competitors that do offer an instant experience.

## 2. No profitable business case for upgrade existing infrastructure

To meet customer expectations, financial service providers are investing in the SCT Inst scheme. In the EU, it is anticipated that this new scheme will take over the current SCT scheme. However, rather than a payments revolution, IP is more an upgrade of the current payments infrastructure. Current SCT payments are in most cases free of charge or available for a small fee (e.g. urgent payments). Since customers already expect this upgrade, it is not likely they are willing to pay (extra) for payments services that are instantly processed through SCT Inst.

## 3. Creation of profitable value-added services is challenging

Offering an upgraded infrastructure to keep up with expectations, is often no basis for a profitable business case. Value-added services on top of IP might be the answer. Instant mobile peer-to-peer (P2P) is a relevant use case and is becoming the go-to service. However, these P2P value-added services have already been claimed by players like PayPal and Tikkie. They already offer these IP services to customers free of charge and on top of the existing payments infrastructure (SCT).

Other services for retail customers are limited, as evidenced by the small number of use cases that circulate across webinars, forums and blogs. This leaves little room for financial service providers to create profitable value-added services on top of the new Instant Payments infrastructure for retail customers.

So, if value-added services aimed at retail customers will not deliver a profitable business case for IP, what will?

## Potential profitable use cases in value-added services for corporate customers

Many SME's and larger corporates (corporate customers) are still lagging in operating instantly. However, also in the corporate space (B2C, C2B and B2B), IP will become the new normal. The potential value of instant payments for these corporate customers is bigger, as they can benefit in multiple ways by

instant incoming and outgoing payments. As such, financial service providers have a window of opportunity to unlock this value by creating new services on top of the IP infrastructure in for instance the following three areas.

### 1. Improve customer service

The ability to send and receive payments instantly allows corporates to interact with their customers in a different way. For example, insurance- and reimbursement claims to customers can be settled in real-time, providing corporates with an instant service level to improve customer experience. On the other side, corporates can offer their customers 'just-in-time' payments. Customers can pay at the latest moment with instant confirmation of successful payment. This new way of interactions with customers can improve customer service.

### 2. Realise operational efficiencies

IP also enables corporate customers in different segments to realise operational efficiencies. Drop shipping business models (e.g. direct delivery from the supplier) are further supported by IP, as merchants can directly forward the customer payment to the supplier along with the order and have goods directly delivered to the customer. The need for holding inventory is therefore reduced.

For merchants, different over-the-counter (OTC) payment methods can be enabled by value-added services on top of the IP. Facilitating Instant credit transfers between merchants and their customers can potentially eliminate the need for third parties (e.g. card schemes). This leads to operational and cost efficiencies.

### 3. Redefine treasury and cash management

As the SCT Inst scheme defines 24/7/365 availability of clearing and settlement, there is no naturally defined cut-off time for making end of day statements. Corporate customers therefore need to redefine their internal procedures for managing cash positions. Also, as incoming payments may take place beyond office hours, corporate customers will need to update their operating capabilities to predict future cash flows in order to optimally manage financial positions overnight and during weekends and holidays.



With adequate tools and services, treasury departments will benefit from the reduced need for operating loans or lines of credit, as payments are not only received faster, but 24/7/365. Efficiency of working capital is increased, as money is faster and at less costs available for reinvestment.

As discussed above, profitable IP use cases are hard to identify for retail customers. Retail customers already expect instant payment processing and are not likely willing to pay (extra) for value-added services. Financial service providers face the risk of losing their customers if they do not meet these expectations.

Value-added IP services for corporate customers, however, are far more promising. IP will also for SME's and corporates become the new normal. In contrast to retail customers, financial services providers still have plenty of opportunities to sustain their relevancy and show their corporate customers how to unlock the IP potential and create value. The time to act is now!

Stay tuned for our next blogs, where we will deep dive on value-added corporate services, like new merchant payment methods, treasury management support and data enriched Instant Payments.



## Authors

Leon Koesoemowidjojo,  
Wouter van den Hengel

[ORIGINAL BLOG](#)[BACK TO INDEX](#)[SUBSCRIBE FOR  
NEWSLETTER](#)

# Decentralised identity enabled by the data control stack turns GDPR into a competitive advantage

David Mintjes on March 19<sup>th</sup> 2018



**David Mintjes**  
Consultant

**GET IN TOUCH**

**A new type of player in the digital identity ecosystem – the consent manager – is enabling customers and organisations to take more control over (identity) data. Relying parties should follow this development with great interest because there are significant benefits gained from joining a data control scheme.**

Exponential growth in the amount of digital transactions and customer data – facilitated by the continued expansion of the internet, the sharing economy and the Internet of Things – brings huge commercial opportunities. In a world where ‘everything’s becoming a transaction’, relying parties realise that collecting this data and translating it into personalised offerings could immensely increase the potential value of their business. However, they are unable to collect and aggregate the appropriate attributes (i.e. data points) from such widely distributed information.

Simultaneously, customers are becoming aware that personal data is stored everywhere, and they expect to have more control over who accesses it. For this reason, regulators are planning to force relying parties to protect personal data in alignment with the new General Data Protection Regulation (GDPR). This will require significant investment on the part of relying parties. Joining a data control scheme can provide a solution which not only enables the relying party to comply with GDPR, but also provides wider access to more accurate customer attributes.



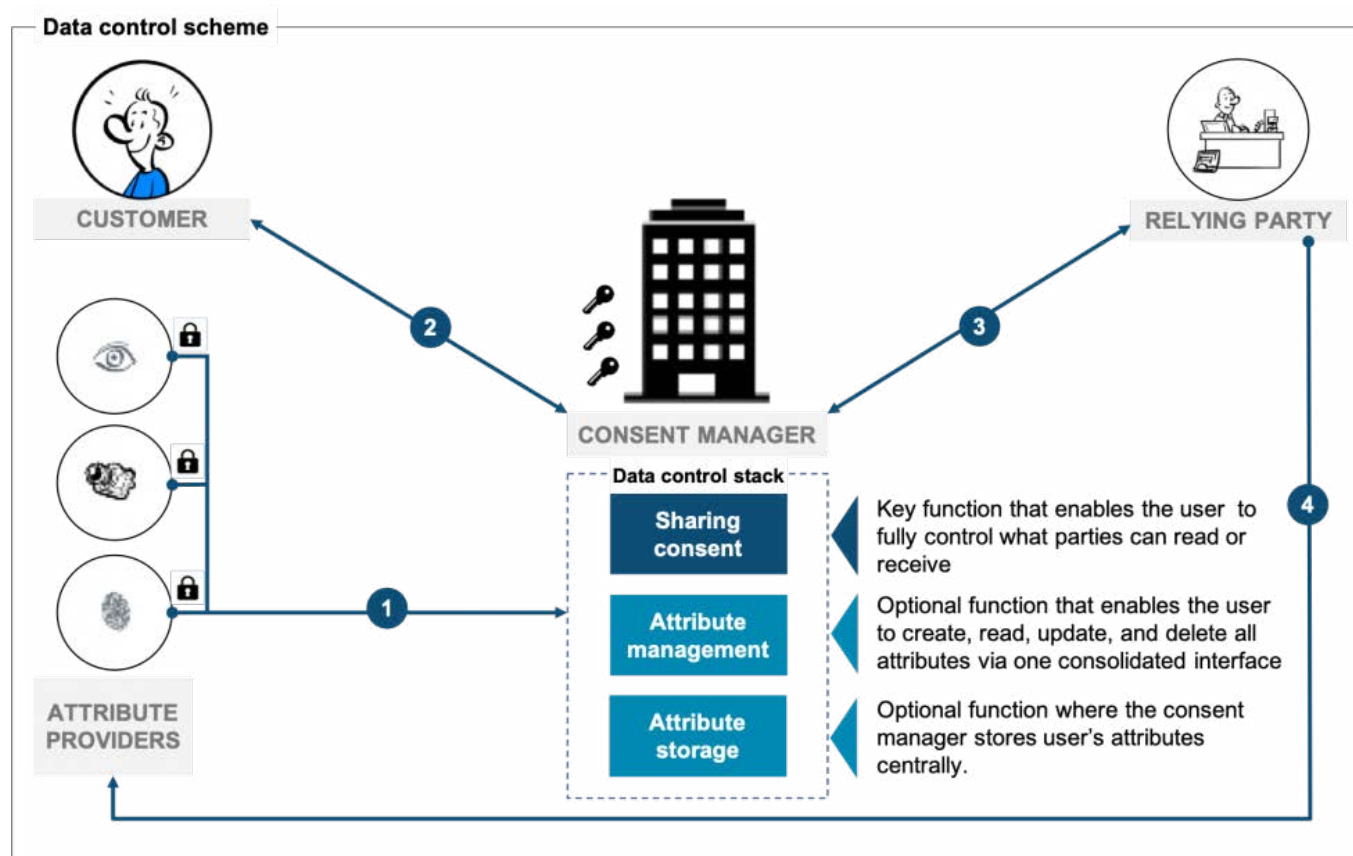


Figure 1.

### How do data control schemes and consent management services work?

Within a data control scheme, the consent manager connects decentralised data from multiple attribute providers with different relying parties. There are four steps as shown in Figure 1.

The consent manager begins by indexing the customer's data from each attribute provider and provides the customer with insights into the available attributes. The customer is now able to modify which parties can access his/her personal data at any time. Consequently, the platform will only share data with relying parties which have explicit customer consent. If these relying parties have updated attributes available that are relevant for other scheme players, they can become attribute providers with new information.

Examples of consent management players include: Dappre (NL), MyDex, Digi.me (UK), Meeco (AU) and Verimi (DE). To be classified as a consent management service, organisations must offer 'consent sharing' as their key service. But the full range of potential services can include:

- **Sharing Consent:** The service which enables customers to fully control which parties can read or receive all their (decentralised) attributes.
- **Attribute management:** The service which enables customers to create, read, update and delete all (decentralised) attributes via one consolidated interface.
- **Attribute storage:** The service which stores customers' attribute data.

The combination of these services provides customers with centralised control over widely distributed decentralised attributes. In the market, we see consent management players choosing to offer a different service mix within the data control stack.

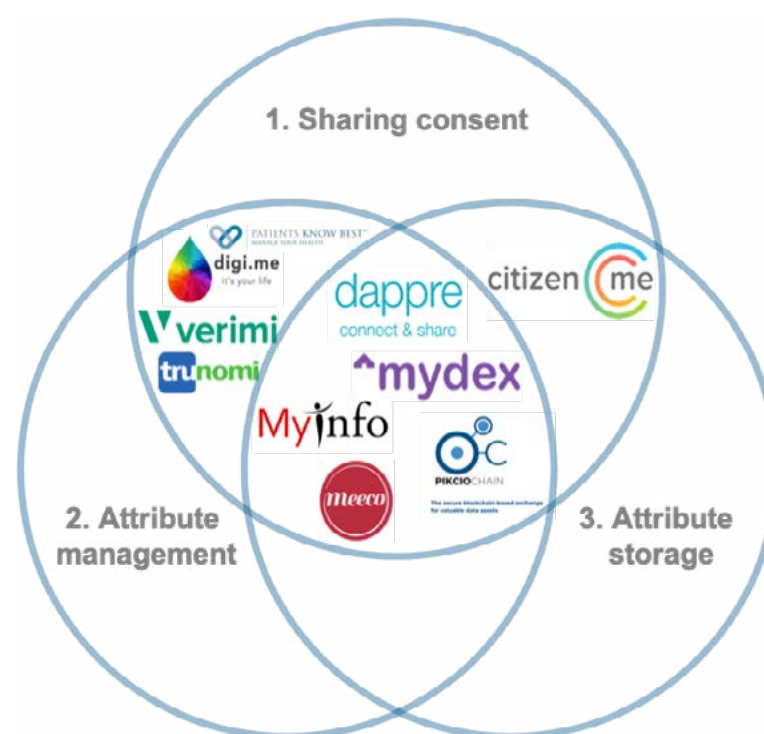


Figure 2.

### Benefits for relying parties

There are three major benefits from joining the right data control scheme:

- By joining forces, relying parties gain **wider access** to attributes and can request a complete set of required attributes from multiple sources.
- Increased customer control over indexed, decentralised personal data ensures a **higher attribute accuracy** because each change at one attribute provider can trigger an update at other parties in the scheme (see step 4 in Figure 1).
- In some cases, the necessity for the relying party to store customer data in-house is removed because consent managers can enable insight into data-points without transferring or duplicating the data. **GDPR obligations** for the relying party can be complied with by using a specialised consent manager.

### Realise competitive advantage through cooperation

Consent managers are enabling customers to take more control over their personal (identity) data. Relying parties, including government, can realise significant benefits by joining a data control scheme and collaborating with like-minded players in the digital transactions ecosystem. In Germany, we already see large relying parties cooperating within the Verimi scheme (e.g. Allianz, Axel Springer, Daimler, Deutsche Bank). Relying parties are able to create competitive advantage through collaborating with partners as more and more value is extracted from decentralised personal data within the scheme. Competitors outside of the scheme cannot access big data unlocked through the scheme, therefore fragmentation of this new two-sided market looms. The scale of this advantage will depend upon whether or not you and your partners can maximise this opportunity.

Are you considering joining forces in a data control scheme? Get in touch. INNOPAY can help you choose the right data control scheme and strategic partnerships.



### Author

David Mintjes

[ORIGINAL BLOG](#)[BACK TO INDEX](#)[SUBSCRIBE FOR  
NEWSLETTER](#)





CYBERSECURITY & PRIVACY

# Customer data: old problems demand new solutions

Shikko Nijland on June 4<sup>th</sup> 2018



**Shikko Nijland**  
CEO and  
Managing Partner

[GET IN TOUCH](#)

## Interested in the Audio version of this article?

**Exponential growth in the amount of digital transactions and customer data is causing organisations to fundamentally review how they will operate in future. As GDPR comes into force, companies need to accept that problems created by their use of customer data now require innovative responses, new ways of more responsible thinking, and an openness to finding collaborative solutions.**

## We risk becoming the 'polluters' of the data sharing ecosystem

"It's like environmental pollution," suggests Shikko Nijland, CEO and managing partner at INNOPAY. "At first everyone thought factories were the way forwards and nobody really cared about the effect on the environment. When we realised there was a problem, we responded by trying to improve the factories, and that's what GDPR is doing – trying to improve the way companies solve legacy problems associated with their use of consumer data."

"GDPR is a good first step, but we also need to think ahead so we can avoid creating new problems in the future. We need to develop cross-sector agreements which will enable all parties in the value chain to benefit from how we exchange and manage data. And this means we need to look for solutions beyond the borders of our own companies."

### GDPR is driving a new level of discussion

Customers are increasingly aware that their personal data has significant value. Shikko: “If you look at digital transactions today, it’s no longer just about the exchange of money for goods. Consumers now understand that the data they provide also has a value for companies. And that’s the reason why GDPR is in place – because data is valuable and you have to take care of it and allow customers to manage it. And this creates liability and exposure for companies.”

“One of the largest changes we’ve noticed is that companies now understand that this data is not their own. In the past, clients would tell us that they owned the data because their customers had given it to them. Now companies are being forced to rethink and take responsibility for the data. And to be honest, I’d be surprised if more than 10% of companies are really prepared for GDPR. Most of them understand the challenges, but solving problems which have built up over several years is extremely challenging. Many of them will be able to tick some of the GDPR boxes, but very few of them will be fully compliant.”

### Don’t centralise data, but centralise access to data

Companies need to change their mind-set. “The winners of tomorrow,” proposes Shikko, “will be those who think from the position of their customers. You need to make sure that every product and every interaction is designed to allow the customer to control his or her data. Companies have a responsibility to provide dashboards which enable their customers to control who uses their data and for what purposes.”

And herein lies the potential flaw in GDPR. As companies rush to create their own local solutions, so the environment risks becoming even more fragmented. Customers will be asked to maintain a separate data dashboard for each individual vendor, leading to time-consuming over-complication and inevitable customer lethargy.

Shikko says, “If companies really want to engage their customers, agreements are needed to allow data to be reused across multiple companies, instead of asking customers to input the same data over and over again. Of course much of this data is already fragmented – we cannot go back in time and change this. But we can begin to manage access to this data more centrally. For example, we can use the ‘digital key boxes’ concept, where customers can assign access to their existing

data to new companies, and also revoke that access on demand. By simplifying and centralising access to data, we can engage customers more effectively, and we can encourage them to use their data in ways which open up new business value for both themselves and for companies. For the first time, value will be added for all players in the data chain.” This may sound simple, but to realise a concept like the digital keybox, it will require collaboration on multiple levels including lawmakers, regulators, companies and consumers. We’ll pick up this ‘digital key boxes’ concept in the next issue of Innsider.

### Collaborative schemes will support more effective data exchange

INNOPAY has proven experience in establishing collaborative data sharing schemes, such as iSHARE for the logistics sector. Shikko adds: “We believe that a crucial part of the establishment of collaborative schemes is the development of communities which will ensure sufficient adoption in the early stages. Most people underestimate the level of investment required in marketing communications during the setup phase. But we’ve seen how crucial it is to engage with multiple industry players from the start – what we call the ‘Coalition of the Willing’. We also believe it is important that the standards which underpin the scheme are formulated by the sector itself. We are the facilitators of the project, but we are agnostic of the schemes themselves. This has to come from the sector or it will be impossible to engage a critical mass of organisations as the scheme is rolled out.”

### Act now to avoid further pollution

Shikko concludes, “We cannot continue as we have done in the past. We already see significant global problems around privacy and who benefits from consumers’ data. These problems will only exacerbate as the amount of data increases exponentially. I’m very concerned that if we don’t tackle the systemic problems today, we will not have the capacity to do so in the future. We’ve seen what’s happening to our world with pollution. This is the scale of problem we could face if we don’t creatively address the challenges of data sharing. We need to think in new ways, to think how to create business value for ourselves and others by working together, and to think responsibly about how the future might look if we fail to act now.”

To discuss how new types of collaborative solutions can solve data sharing challenges and create new business value for your organisation, feel free to contact Shikko.

**Author**

Shikko Nijland

[ORIGINAL BLOG](#)

[BACK TO INDEX](#)

[SUBSCRIBE FOR  
NEWSLETTER](#)



# Looking for the missing part of GDPR: a 'soft infrastructure' for sharing your data

Shikko Nijland, Douwe Lycklama on July 3<sup>rd</sup> 2018



**Shikko Nijland**  
CEO and  
Managing Partner

[GET IN TOUCH](#)



**Douwe Lycklama**  
Founding Partner

[GET IN TOUCH](#)

**GDPR mandates that organisations must provide consumers with increased levels of visibility and control over their personal data. But this data is already fragmented across the farthest reaches of the internet, and the long-term needs of neither consumers nor corporates will be served by the implementation of local dashboards and consent management apps by each player in the chain. INNOPAY proposes a collaborative approach to solving this challenge which will deliver convenience and control to consumers, and both GDPR compliance and new business opportunities for companies.**

## **Data consent and sharing can be solved with proven solutions**

Pollution of our oceans quietly crept up on the world, scarcely noticed by most of us until our eyes were opened to the widespread contamination of marine life which will only be resolved by systemic changes in waste management. The fragmentation of personal data can be understood in similar terms; we have gradually created an endemic problem which has recently been spotlighted by our growing understanding of the value of personal data. Now we need to work together to implement a new type of collaborative solution which can be seen a 'soft' infrastructure as it does not involve physical elements per se.

GDPR provides a strong regulatory response to the challenge, with its focus on handing back control of personal data to consumers through stricter controls. Even though consumers have additional powers of control, many people will find the process of

managing and sharing fragmented data across multiple organisations both complex and time-consuming, if possible at all. Data sharing and consent is the next 'many to many' problem resulting from digitisation of transactional services. Other examples are internet, GSM, payments, digital identity, electronic invoicing and EV car charging payments. All services powered by a 'soft' infrastructure leading to 'many to many' interoperability.

So the challenge is to provide a context in which this new-found 'many to many' control becomes practical and manageable. And the answer is unlikely to be provided by single repository 'data vault' solutions due to the significant administrative overhead and the additional risk of single point of failure.

#### **The solution lies in collaboration on a practical level**

Instead of attempting to centralise consumers' data, the Digital Key Box principle leaves the data at source, and focuses on providing aggregated access and management of that data. In practical terms, it will provide consumers with a simple and effective means to manage consent and allow data sharing across organisations. And if implemented properly and adopted widely, it will also create significant commercial opportunities for businesses, whilst simultaneously ensuring they are fully compliant with GDPR.

The concept has an elegant simplicity. As a consumer, you have already provided data about many aspects of your personal and professional life to multiple organisations, such as your bank. So a key box at your bank, telco or insurer, in which a separate digital key is associated with each personal data attribute, could provide a perfect hub to control and manage your data. Also data residing at other sources. When a 3rd party requests your data, for example an insurance company needing personal details to provide a quote, you simply give consent with bespoke conditions (eg reason, number of uses) to use the relevant keys to unlock access. If at any future time, you wish to revoke the 3rd party's access to your data, you simply withdraw the digital key through the dashboard of the key box. From the consumer's

point of view, the system can be made easy to use and provides the level of control envisioned by GDPR.

#### **Not moving strengthens digital incumbents**

Commercial organisations will also benefit from the Digital Key Box concept. A new role of Consent Manager is rapidly beginning to emerge, and several (start up) companies (e.g. Verimi, Digi.me, Meeco, Trunomi, Mydex, Peercraft) strive to occupy this central position in consumers' lives. Most of the actors endorse the need for interoperability and several EU Horizon initiatives can be expected to address this topic. The Qiy Foundation advocates for such an interoperable infrastructure for personal data already for a decade. The recent iSHARE data sharing initiative applies similar infrastructure principles but is wholly focussed on business to business data, launching in the logistics sector in 2018.

Big data organisations (GAFAM) have the head start as they already offer comprehensive dashboard services on the data users have shared with third parties. In the 'permissions' screens user can actively manage consents given, e.g. when logging in with an existing account. Such solutions should also become part of the 'soft' infrastructure, instead of them becoming THE infrastructure.

Companies holding personal data will also be able to create new relevancy for their customers, not only by providing effective hubs for managing access to personal data, but also by using the new levels of trust which consumers will experience. If a consumer feels secure in the knowledge that he can effectively control his personal data, he is more likely to consider offering that data more widely, and enriching basic data with additional information about personal preferences. So by offering incentives, companies will be able to access far greater volumes of relevant and marketable data than in the past. And in a world where data is emerging as the new global currency, and digital transactions are at the heart of everything we do, this will open up significant new opportunities for insightful organisations.



### Guiding the way forwards with trust and cooperation

A so called 'soft' infrastructure is required to facilitate the Digital Key Box scheme, just as with any physical infrastructure system. We don't build rail or road networks for only one town; we create one consolidated system which serves all users across a country and even national borders. We propose adopting the same principle with personal data sharing and consent management, just has been done with e.g. internet, GSM, payments, digital identity and electronic invoicing.

In practice, this requires the co-creation of a framework of agreements across various technical, functional, legal, business and organisational domains. A trusted technical

infrastructure would need to be established to allow key boxes to communicate. Agreements would be required across a wide range of stakeholders on fundamental issues such as the appropriate parameters of consent management. The challenges are significant but certainly not insurmountable. INNOPAY has a wealth of experience of guiding and facilitating these types of schemes, and bringing together coalitions of key organisations to co-create solutions which are driven by the sectors and industries which will deploy them.

To discuss how the Digital Key Box principle can solve data sharing challenges and create new business value for your organisation, feel free to contact the authors.



### Authors

Shikko Nijland, Douwe Lycklama

[ORIGINAL BLOG](#)[BACK TO INDEX](#)[SUBSCRIBE FOR  
NEWSLETTER](#)

# Quantum computers will revolutionize cryptography and cybersecurity. Here's why.

Krijn Reijnders on November 20<sup>th</sup> 2018



**Krijn Reijnders**  
Business Analyst

[GET IN TOUCH](#)



**Jelger Groenland**  
Senior Manager &  
Cybersecurity Lead

[GET IN TOUCH](#)

**Sufficiently strong quantum computers will seriously disrupt the confidentiality and integrity of secure digital communication everywhere. They will effectively break most of the current methods to securely exchange data, and quantum-resistant alternatives are not yet mature. Even though the development of such quantum computers may take years, you are running risks you are not aware of. In this blog, we will explain how quantum computers will revolutionize your data security and why you should be aware and prepare.**

Data is everywhere, and everyone is sharing data. If you want to securely share and exchange data, proper data security is fundamental. One of the pillars of data security is cryptography, the practice of encrypting and decrypting data using cryptosystems to enable secure communication. But the development of quantum computers is weakening this pillar: it's showing cracks already.



## Quantum computers will break current cryptosystems

A quantum computer with enough computing power would shatter the current security of public key cryptosystems (see frame A) upon which the digital exchange of data is based. The security of these cryptosystems is based on only a few mathematical problems (see frame B below). Our trust in digital security relies upon the fact that up until today no one has been able to solve these problems efficiently. A paper by Peter Shor, written in 1994, explains how a quantum computer would be able to do so. The development of quantum computers has seen quite a bit of progression in recent years, with IBM reaching 50, Intel 49 and Google even 72 qubits. Estimating when a large enough quantum computer arrives remains difficult. However, experts <sup>1</sup> agree that we should start looking at how to prepare for such an arrival. By discussing three fundamental questions, we will explore this world of Post Quantum Cryptography (PQC).

### A. Quick introduction to cryptosystems

There are two main branches of cryptography that we use to ensure safe exchange of data.

#### 1. Symmetric cryptography

In symmetric cryptography two parties exchange data using the same encryption key. Party A encrypts his data using some key X, party B decrypts this data using this same key X. Symmetric cryptography is fast, but the problem is exchanging the key, which needs to be done before any encrypted exchange can ensue.

#### 2. Asymmetric cryptography

In asymmetric cryptography (public-key cryptography), the two parties use different keys to exchange data. By some nifty mathematics, this enables a secure exchange of data without the need to exchange a key first. The downside is that asymmetric cryptography is slow in comparison to symmetric cryptography.

In general, to exchange data we use asymmetric cryptography to exchange the key that will be used in symmetric cryptography. However, this carries the risk that “breaking” asymmetric cryptography also “breaks” this key exchange for symmetric cryptography.

### B. Current asymmetric cryptosystems

The two main current approaches to asymmetric cryptography are RSA and ECC. There are some differences between these two approaches: The security of RSA is based on the mathematical problem of finding divisors of numbers, i.e. finding that 5 divides 15; the factoring problem. This problem is easy for small numbers but becomes very hard when the number is very large. ECC bases its security on a problem that is a bit harder to explain: the elliptic curve discrete logarithm problem (ECDLP). In practice, the difference between these two approaches lies in the length of the key. To achieve the same security against current attacks, RSA needs keys that are much larger than ECC needs. ECC is therefore preferred in applications where processing power is limited.

Both the factoring problem and ECDLP are efficiently solved by quantum computers, with current research indicating that ECDLP will be the easiest of these two to be attacked by a quantum computer.

#### 1. How will we securely exchange data in a world with quantum computers?

In a quantum world, we will exchange data securely using new cryptosystems, that replace the currently used ones. To ensure that we have such quantum-resistant cryptosystems in the (near) future, the National Institute of Standards and Technology (NIST), an authority on cryptosystems, initiated a process to develop, analyse and standardise such systems. Their goal is to release quantum-secure standards somewhere in 2022/2024 <sup>2</sup>, built on mathematical problems that quantum computers cannot solve efficiently. Such cryptosystems should enable us to securely exchange data in a world with quantum computers.

#### 2. What do we need to securely transition to these new cryptosystems?

To prepare for this transition, we’ll need to analyse which systems currently use what cryptographical standards and to what standards they need to be upgraded. Security experts will need to be educated on these new standards and will need to know how they should be implemented. Much of this work can already be started, to ensure that this time-consuming transition would be completed before we start running major security risks. This is comparable to the Y2K problem; a race against the clock. Therefore, some experts call this transitioning problem and the time until quantum computers Y2Q (years to quantum).

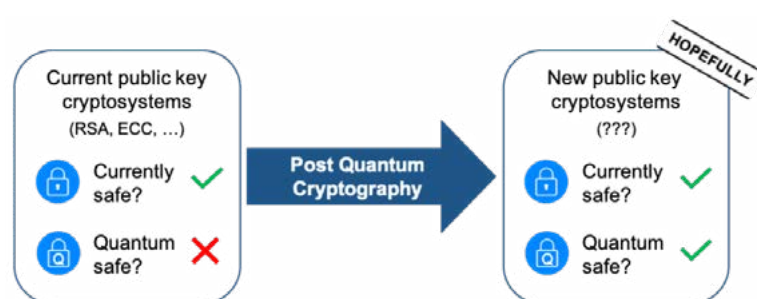


Figure 1.

### 3. Why is the exchange of highly secure data at risk today?

Even if we transition into these new (hopefully) quantum-resistant cryptosystems in time, there is a more urgent issue we should address. Imagine a malevolent party saving loads of your encrypted data today. They (the party) keep this data stored somewhere until they have access to a quantum computer that is strong enough to decrypt this data. Quickly they will have a huge pile of your data in which they might find nuggets that were meant to be secure for decades, with an impact on your business. Although such a quantum computer may lie more than a decade away, this poses a threat for highly secure data today. If you have data which needs to remain private for years, you need to start thinking about how you store and exchange that data now.

#### What you can do to be aware and prepare for Y2Q.

So, there we have it. There is currently no great long-term option to exchange highly secure data. The transition into new cryptosystems will take huge amounts of time, effort and resources. Even then, trust in these new systems will need time to develop. But there are some things that we can do already:

4. Look at using hybrids of current cryptostandards and new cryptostandards;
5. Catalogue how you use current cryptostandards in your systems and products;
6. Develop a strategy for the transition into these new cryptostandards, specifically when developing long-term products which use quantum-vulnerable cryptography
7. Develop knowledge in the area of post quantum cryptography, which will be a necessity in coming years;
8. Carefully analyse the different sensitivities of different sets of data. Then adapt your data exchange security to that, especially for data that needs to stay secure for more than 5 years.

We do not know when a large enough quantum computer will be ready. But we do know that doing nothing is not an option.

If you would like to know more about how post-quantum cryptography or how cryptography can help protect your organisation, please contact the authors.

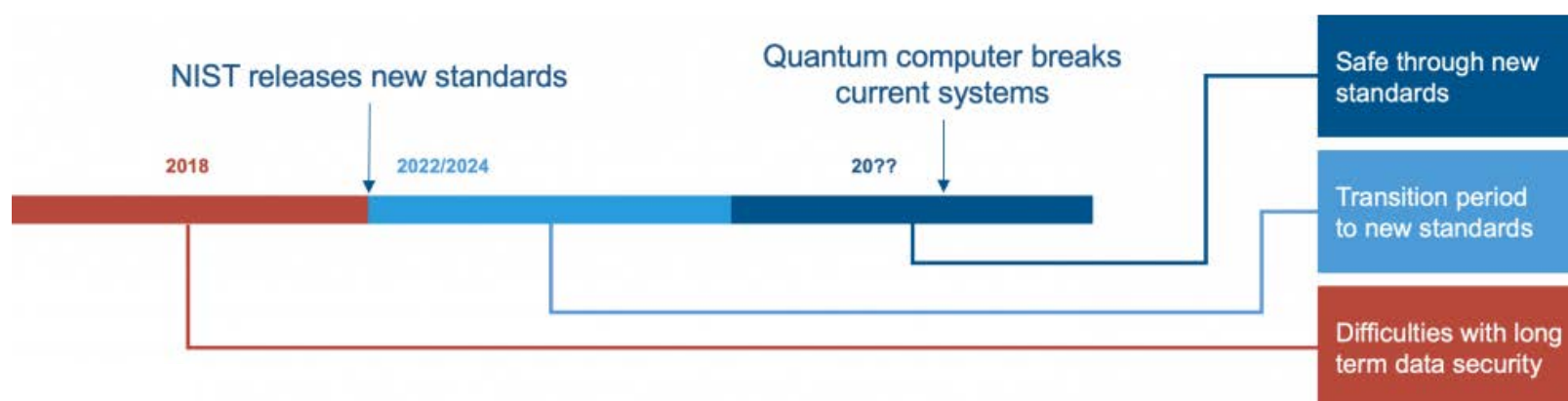


Figure 2.

1. Dr. Michele Mosca estimated the chance that a cryptosystem will be broken before 2026 as one in seven, and before 2031 as one in two. He calls this moment Y2Q (Years 2 Quantum). He made these estimates in 2016, before the major advancement in numbers of qubits by IBM, Intel and Google were made public.
2. Source: <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline>

**Author**

Krijn Reijnders

[ORIGINAL BLOG](#)

[BACK TO INDEX](#)

[SUBSCRIBE FOR  
NEWSLETTER](#)





PSD2 & OPEN BANKING

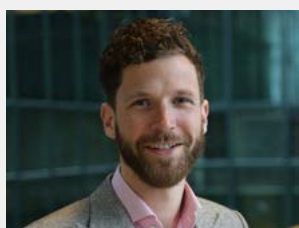
# Mastering Open Banking: How the 'Masters in Openness' create value

Mounaim Cortet, Art Stevens on September 19<sup>th</sup> 2018



**Mounaim Cortet**  
Senior Manager and  
Lead Strategy

GET IN TOUCH



**Art Stevens**  
Consultant

GET IN TOUCH

Senior bank executives are starting to understand that Open Banking will have key implications on their future competitive positioning and related digital transformation activities. We define Open Banking as a business approach in which value creation results from sharing, providing and leveraging access to bank resources through application programming interfaces (APIs). This way data, processes and other business capabilities of banks are made available to an ecosystem of (selected) third parties (e.g. fintechs, technology vendors, corporate customers).

## Introduction

Open Banking is set to transform digital experiences through compelling value propositions developed by third parties leveraging access to bank resources, ultimately adding value and putting the customer more in control. Banks that are able to put the required capabilities in place to effectively and seamlessly engage with third parties will benefit from an early mover advantage.

In this article we assess **four core API Developer Portal capabilities** of 50+ banks and define **five strategic actions** that banks can undertake to execute their Open Banking strategy.

In the capability assessment we focus on specific aspects of the Open Banking strategy, that is, the functional richness of APIs offered (i.e. Functional Scope) and the extent to which third parties are able to interact with these APIs in a seamless manner (i.e. Developer Experience). The bank's API Developer Portal is where these aspects come together.

#### **Four core API Developer Portal capabilities**

Open Banking is definitely not a business model fit for all types of banks. The extent to which an Open Banking play will be successful depends on many different aspects that banks need to get right. This includes its Open Banking strategy, taking into account existing product offering, competitive positioning and size of customer base, and the bank's ability to execute on that strategy.

Many banks are taking action to engage and support external developers through an API Developer Portal. However, the level of maturity differs considerably across banks, as we assess in the **INNOPAY Open Banking Monitor (OBM)**. Banks differ on four core capabilities: API Catalogue, API Documentation, Developer Usability and Developer Community. While the majority of banks is still mainly working on 'getting the basics right' of their Developer Portal, we also observe that others are gradually expanding the functional scope of their API portfolio.

#### **Five strategic actions to execute on your Open Banking strategy**

With many banks across the globe establishing the basics of their API Developer Portal, there is a strong incentive towards differentiation in the emerging Open Banking landscape. To ensure banks are prepared for this new landscape, we have defined five strategic actions: 1) Learn from global API best practices across industries, 2) Develop API rationale and strategy for your business to create new avenues for revenue growth, 3) Identify and prioritise the value that can be captured with APIs, 4) Manage API monetisation actively by determining if, what, how and who to charge in a transparent manner, and 5) Drive usage and adoption of your APIs to accelerate network effects and gain scale.

Open Banking should be approached as a business strategy and model in its own right, requiring an alternative way of thinking and working in product development. Combined with powerful execution capabilities and a successful and scaled partnership ecosystem banks will be able to future-proof their competitive position in the Open Banking era.

This article is structured as follows:

1. Introduction: INNOPAY Open Banking Monitor shows that Open Banking is gaining traction
2. API Catalogue
3. API Documentation
4. Developer Usability
5. Developer Community
6. Five actions to execute on your Open Banking strategy<sup>1</sup>.

#### **1. Introduction: INNOPAY Open Banking Monitor shows that Open Banking is gaining traction**

Banks across the globe are starting to understand that Open Banking will have key implications on their future competitive positioning and related digital transformation activities. Open Banking has reached the boardroom agenda and strategic investments are being made or at least considered.

The evolutionary journey towards Open Banking is driven by ongoing digitisation of financial services, as depicted in figure 1.

In this article we define and focus on Open Banking as a business approach in which value creation results from sharing, providing and leveraging access to bank resources. This in contrast to just owning these resources and being closed. Data, processes and other business capabilities of banks are made available to an ecosystem of (selected) 3rd parties (e.g. fintechs, technology vendors, corporate customers) through application programming interfaces (APIs).

Open Banking is set to transform digital experiences by enabling third parties to develop compelling value propositions while leveraging access to bank resources and putting the customer more in control. As the benefits materialise at scale we will witness an accelerated shift towards Open Banking platforms. These platforms enable banks to effectively and securely interact and co-create with an ecosystem of service providers through APIs. Both banks and these service providers can create benefits for their mutual customers, strengthen their competitive position in the API economy and potentially establish new avenues for revenue growth. For banks this could offset competitive pressure resulting from the increasing openness in payments and banking introduced by PSD2. Indeed, in Europe, we already observe that banks are starting to experiment with offering APIs beyond the (perceived) mandatory functionality under PSD2.



## Open Banking is not fit for all banks

Open Banking is definitely not a business model fit for all types of banks. The extent to which an Open Banking play will be successful depends on many different aspects that banks need to get right. This includes its Open Banking strategy, taking into account existing product portfolio, competitive positioning and size of customer base, and the bank's ability to execute on that strategy. In this article, we focus on specific aspects of the strategy, that is, the functional richness of APIs offered and the extent to which third parties are able to interact with these APIs in a seamless manner. The level of maturity differs considerably across banks on these aspects, as we have assessed in a prior release of the **INNOPAY Open Banking Monitor (OBM) "Who are the Masters in Openness?"**. Note that the level of openness of a bank is relative to the bank's product portfolio, that is, larger banks tend to have a more comprehensive product catalogue. As this study measures absolute openness, these elements (i.e. reach and product portfolio) should be kept in mind.

## Strong API Developer Portal capabilities are key to winning in Open Banking

A winning strategy is quintessential for banks to effectively participate in the Open Banking platform game. While there are little precedents in banking, banks can learn from open business models that have revolutionised other industries. Indeed, a selected number of progressive banks are starting to engage by publicly launching their own Developer Portals including APIs and sandbox environments. These capabilities allow banks to offer secure and controlled access to third parties to interact

and use the bank's functionality and customer's data to create next generation financial services. Banks that are able to put the required capabilities in place to effectively and seamlessly **engage with third parties**, and facilitate an Open Banking ecosystem through its platform, will benefit from an early mover advantage. This will in turn strengthen the bank's API offering and a supportive ecosystem of third parties that drive customer value creation. Many banks are taking action to engage and support external developers through a comprehensive Developer Portal to facilitate effective interaction.

## INNOPAY Open Banking Monitor assesses API Developer Portal Capabilities

The initial OBM assessment conducted early March 2018 included Developer Portals across the globe and triggered many positive reactions from various banks and financial institutions worldwide. The OBM has proven to be an accessible and intuitive tool providing a snapshot of the current state of play regarding API Developer Portals and insight in a bank's relative position. In this initial release, we have seen that the majority of banks mainly worked on 'getting the basics right' of their Developer Portal, rather than the Functional Scope of their API portfolio.

In this second release, 'OBM 2.0', INNOPAY's assessment has been enriched with new banks, new API functionality and new features that drive the Developer Experience and nurture the use of APIs to accelerate innovation in financial services. Figure 2 depicts the updated benchmark results.

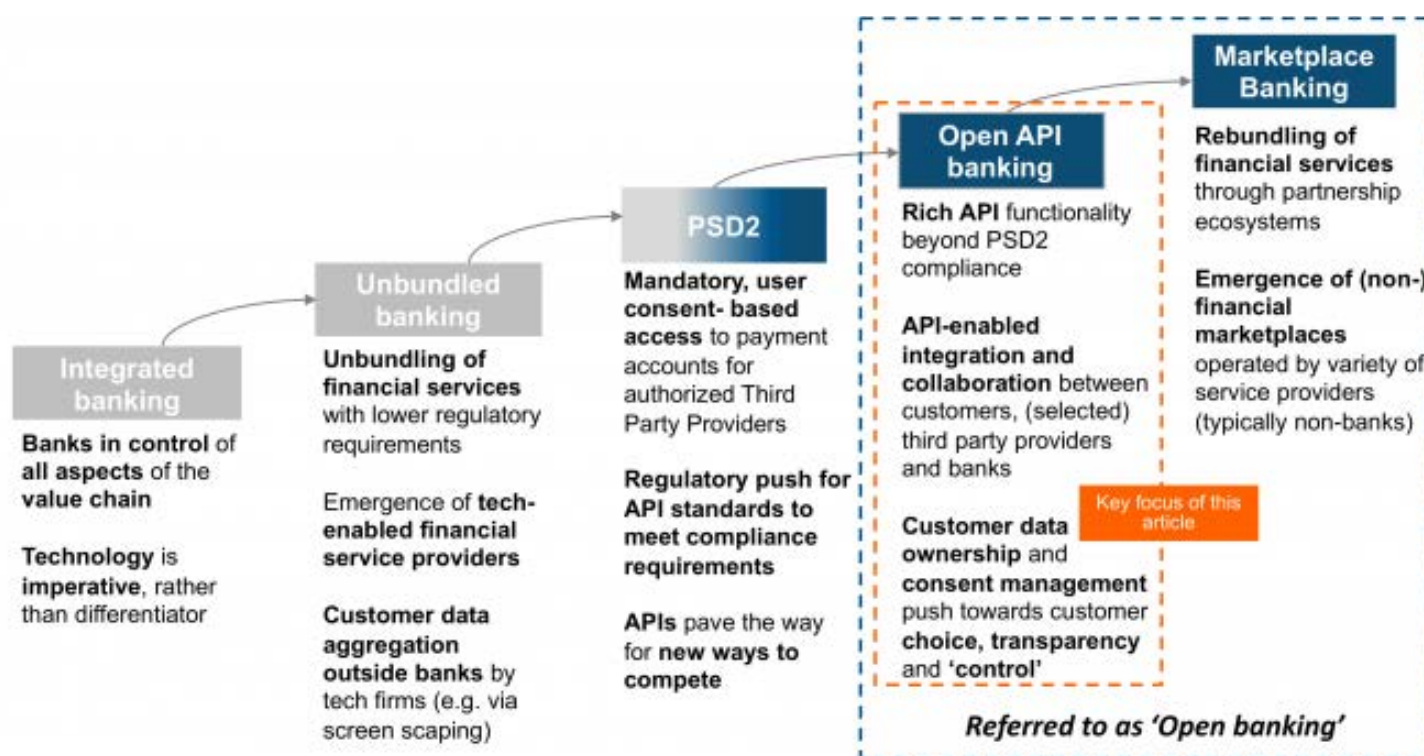


Figure 1.

OBM 2.0 evaluates the relative position of banks across four core Open Banking platform capabilities, as depicted in figure 3 below. The state of play and best practices across these core capabilities will be further elaborated in the remainder of this paper.

## 2. API Catalogue

Key messages on API Catalogue:

- *Becoming a Master in Openness is about relative openness rather than absolute openness, meaning challenger banks and incumbent banks can only open up the resources they have. Therefore, the functionality the API enables is a better indicator of openness, rather than the number of APIs*
- *Current Open banking approach will lead to fragmented API Catalogues roadmap; guidelines in API design could improve the growth of the Open Banking ecosystem, increasing scalability and cohesion between banks and 3rd parties*
- *The design of API functionality varies with the granularity offered and can range from "do it yourself" to "ready to assemble" functionality*

The API Catalogue is referring to all the products banks are exposing through APIs. In Europe, many banks are responding to the PSD2 compliance challenge by offering APIs enabling the mandatory services (i.e. Payment initiation, Account information and Confirmation of funds availability). We already observe some leading banks that are extending their offering by exposing more API functionalities to serve 3rd parties and corporate customers directly. Banks outside Europe are also starting to open up, seeking to expose functionality and data through APIs to add value to their Open Banking ecosystem.

## Current Open banking approach will lead to fragmented API Catalogues

API functionality can be designed and built in various ways, and the decision to expose certain APIs is determined by the bank's strategy. There seems to be no general structure on how the various banks define and set-up the Functional Scope of their API offering (i.e. API Roadmap). Common API standards for the Functional Scope could, however, promote **growth of the Open Banking ecosystem**. Currently, both the content (what is actually offered) and the delivery (the way in which it is offered) differs to a large extent per bank, increasing the risk of fragmentation. In Europe, however, we do see some early



Figure 3.



Figure 2: INNOPAY, Open Banking Monitor (OBM) 2.0 - Developer Portal benchmark (update Sept 2018).



signs of convergence with numerous banks offering PSD2 inspired functionality (e.g. account information services and payment initiation services) according to the **NextGenPSD2 API framework** of the Berlin group. While this framework provides for a good start, NextGenPSD2 is an API framework and not a single standard such as **Open Banking UK**. Put simply, the API framework provides a toolkit for banks to build their own PSD2 API standard, allowing for various degree of freedom on certain API design aspects. Creating common API standards in an early stage for a community of (small) banks in a particular region could contribute to a faster growing ecosystem and increased cross-fertilisation.

Figure 4 below shows the division of the number of measured API functionalities per category currently observed in the Open Banking landscape. Just over 50 banks with publicly available Developer Portals (in the English language) were examined, spanning different types of banks (i.e. majority incumbent and one fifth challenger banks) and types of business (i.e. retail and wholesale) to create an insightful overview of the current state of play in Open Banking. To define API functionality, we compared corresponding APIs of different banks with the possibilities they offer. One API can hold one or more functionalities, next paragraph will elaborate on this.

On the right side the categories are explained and the top 3 most common API functionalities per category are shown. This top 3 provides insight on which functionalities are most commonly offered across banks. Most offered functionalities are related to reading information (e.g. GET Account Balance) from the user's account instead of writing (e.g. POST SEPA Credit Transfer). As banks grow accustomed to Open Banking, more write functionalities are expected to emerge in parallel.

There is also a range of miscellaneous API functionalities that is offered by a single or very few banks, which are not taken into

account in figure 4. These API functionalities vary greatly and are still in an emerging state. If these offerings mature they can be reported in a future OBM release.

**API functionality is a better indicator for openness, than the number of APIs**

The various banks with a Developer Portal are often ranked by the number of APIs they are exposing. In our research, we are using the number of API functionalities instead, because due to the fact that an API can have one or more functionalities, comparing number of APIs would not give a clear representation of what the bank actually offers. Our analysis shows that a particular 'Bank A' can have a single comprehensive API for transaction history incorporating various functionalities, where 'Bank B' offers a single API for transaction history of payment accounts, another API for card payment transactions, another API for sent transactions and a separate API for incoming transactions. While both banks are offering the same functionality, Bank B would (unfairly) score higher when number of APIs would be considered a leading indicator for the extent of openness.

**Becoming a Master in Openness is about relative openness, not absolute openness**

Challenger banks and incumbent banks can only open up the resources they have. Being a true Master in Openness is more about relative openness (which % of functionality does the respective bank open up), rather than absolute openness (how many functionalities does the respective bank open up). The Open Banking Monitor measures absolute openness, therefore the results of challenger banks need to be interpreted with caution especially when comparing these to incumbent banks.

Where, in our previous release of the OBM, we observed many challenger banks leading the ranks on Functional Scope (i.e. Bunq, Starling and Fidor), we observe that incumbents are catching up. The top performers on API Catalogue, i.e. Functional

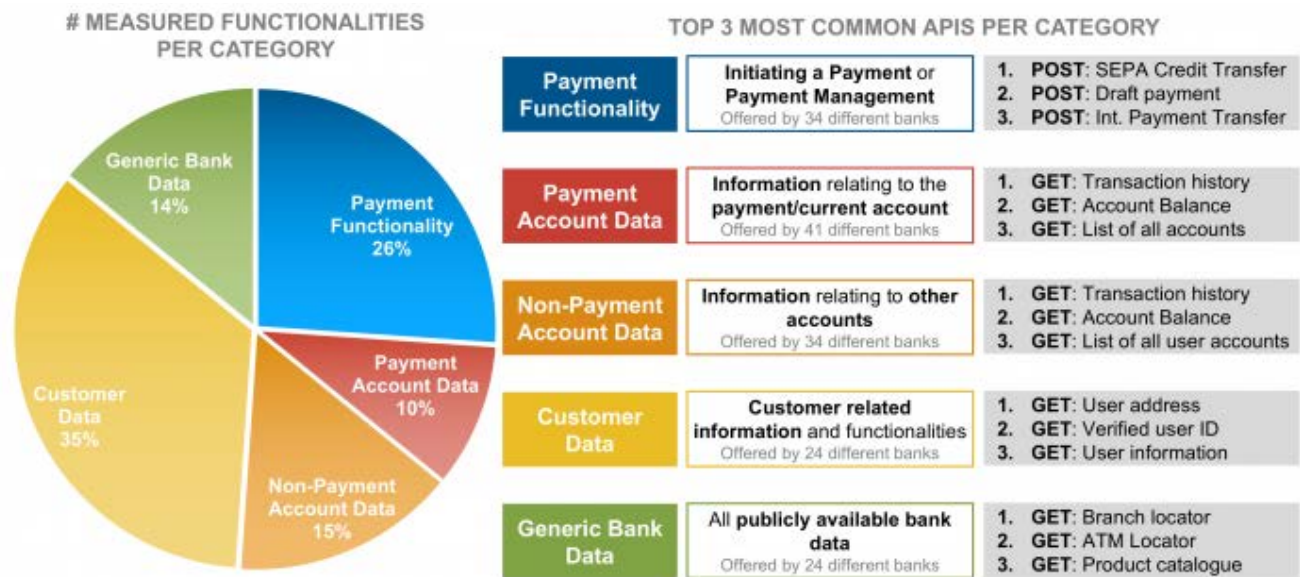


Figure 4.



Scope, in this release are large banks with a clear focus on Open Banking, such as DBS, BBVA and ERSTE Group. BBVA offers a very comprehensive account functionality spanning multiple account types (e.g. savings, checking etc.). DBS offers five different ways of payment/transfer methods (including instant payment) and extensive payment management options (e.g. merchant checkout, corporate bill payments and refund/chargeback management options).

**Different regions show a preference for certain categories**

Figure 5 below shows an overview of the various API functionalities that are available across certain regions. The figure shows that based on our research Europe is leading the

Open Banking development in general and embracing Open Banking even beyond the mandatory PSD2 APIs. It seems that Oceania is experimenting with Open Banking by offering APIs like “Branch locator” and “Product catalogue”. Singapore seems to show high numbers of the category “Generic Bank Data”, although since the number of participating banks in Singapore is rather low, it is hard to make any reasonable statements on the Asia region. Overall, Oceania and US seem to be lagging behind in the variation of API functionalities in comparison to the offering of banks in other regions.

Figure 6 below shows a more detailed view of the number of API functionalities per category offered by the top 10 banks in the

Open Banking landscape. Banks in Singapore are embracing Open Banking and offering the most functionality. As stated above and emphasised by the marginally presence of only two challenger banks in the top 10; challengers are lacking in Functional Scope, presumably due to their minimal product offering. There seems to be great variation in the offering of functionality. Some offer fine grained functionalities (i.e. Bunq),

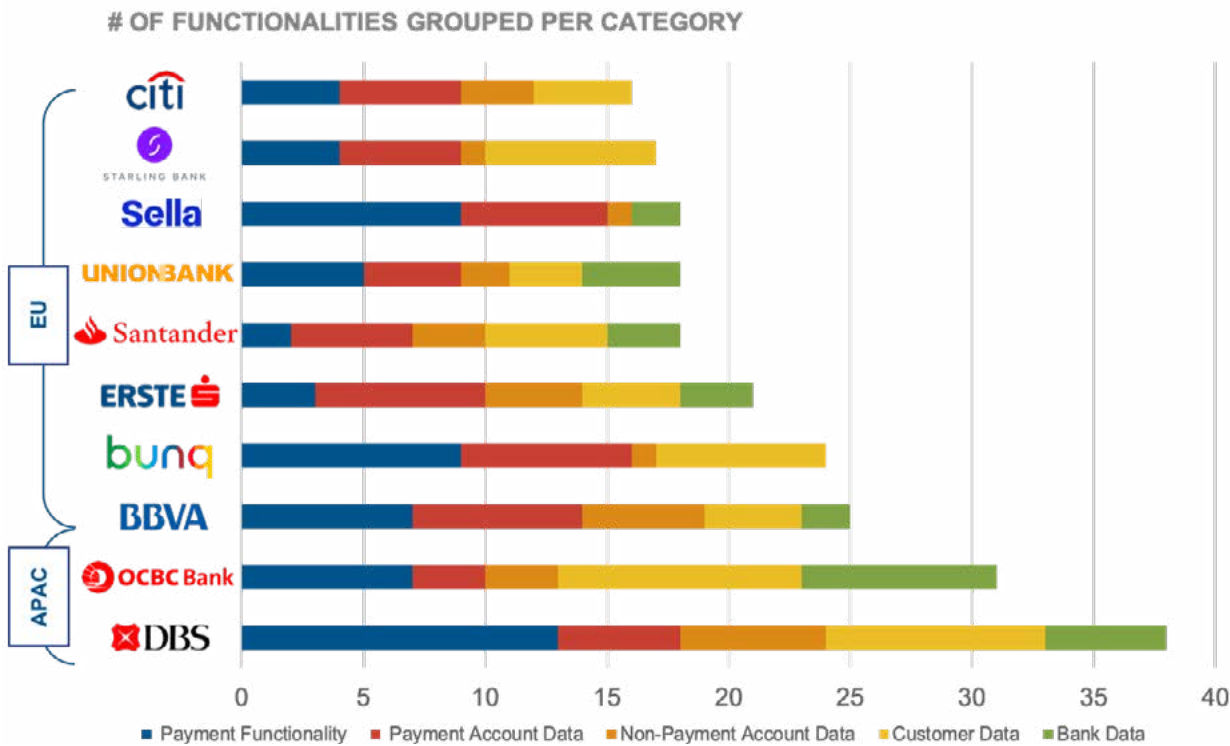


Figure 6.

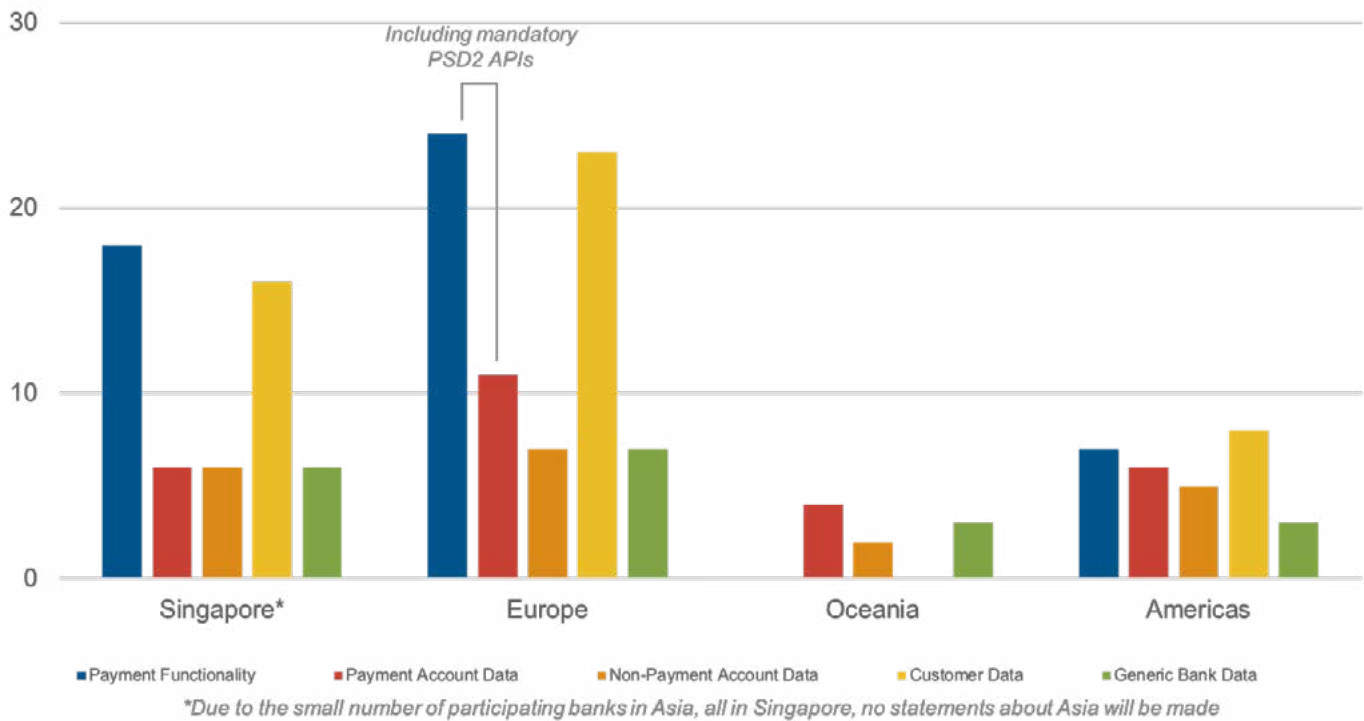


Figure 5.

some offer full serviced products (i.e. BBVA), this will be further elaborated in the next paragraph elaborating on API design.

Design of APIs varies with the granularity offered

We observe a great variety and granularity in API functionality offered by banks, as shown in figure 7. The figure outlines the approach banks can have on building their API offering. These approaches range from “do it yourself” to “ready to assemble” APIs on the other end of the spectrum with potentially many hybrid forms in between.

For banks, it is relevant to determine who the target group is that will be consuming the API and for which purpose. The API fit gives a representation of the type of bank and the desired granularity of the API. Assessing the desired granularity of the functionality will allow banks to conclude which design and structure will be most suitable for their APIs.

3. API Documentation

Key messages on API Documentation:

- Clear and unambiguous API Documentation is essential to enable API consumers to build efficient connections and facilitate self-service
- Banks differ in quality of API Documentation offered, with main difference in accuracy and comprehensiveness
- Good API Documentation will support the marketing of APIs

The core capability “API Documentation” refers to the quality, comprehensiveness and(logical)structureofthedocumentation of the complete API offering of a particular bank. API Documentation is needed for developers to understand the structure of the API, which data fields are used and, which parameters can be used to use an API functionality.

API Documentation shows considerable difference in structure and quality

As with the previous release of the OBM, there are considerable differences between the way documentation is offered and functionality is being added for developers to get acquainted with the bank’s APIs more quickly. Although it is obvious that all APIs and their functionalities need to be properly documented in order to drive usage, banks seem to be struggling to get this right. The top 3 banks in API

Documentation, BBVA, Nordea and ING, all have elaborate explanations of all attributes used in the APIs. Version history of the APIs seems to be missing for some banks, but this could be explained by the fact that their Developer Portals are only just recently launched.

Figure 8 shows a comparison of two different Developer Portals offering API Documentation for a ‘GET Transaction history’ API. This example illustrates opposite ends of a spectrum of how API documentation is structured by banks.

Main differences between the API documentation of bank A and bank B is the overall structure and the description of each field. Bank A has clearly defined which fields are returned, by offering a comprehensive explanation of each parameter; what its object type is, the description of its contents, an example value and whether the field is required or returned optionally. Bank B gives little to no description of the returned values, leaving it up to the developer to guess what values he is actually receiving. It can be stated that Bank A helps developers to get started more quickly, since the returned attributes are clearly documented and therefore the developer knows how to use it and what to expect.



	Do it yourself	Ready-to-assemble
		
Description	<ul style="list-style-type: none"><li>- Start without a pre-developed plan</li><li>- Everything needs to be designed, sorted and built</li><li>- Starting with pieces of wood, a saw and pipes will be the equivalent of the stripped functionality like schedule and capture payment</li><li>- Mostly single functionality per API</li></ul>	<ul style="list-style-type: none"><li>- Build according to the banks plan, using building blocks</li><li>- There is a structured plan for every single cabinet or drawer, however, the total kitchen needs to be designed</li><li>- Building kit reduces the possibilities compared to DIY however, less self-inventing will be needed</li><li>- Most APIs hold multiple functionalities</li></ul>
API Consumer pros	<ul style="list-style-type: none"><li>- Increased flexibilities using combinations (parts of) of APIs</li><li>- Efficient APIs can be built, by incorporating only the necessary single functionality</li></ul>	<ul style="list-style-type: none"><li>- More possibilities with less creativity</li><li>- Ready to use off the shelf APIs</li></ul>
API Consumer cons	<ul style="list-style-type: none"><li>- Insights in bank processes is required to build APIs (e.g. the steps in the payment process)</li><li>- More work to create apps, since several functionalities need to be combined</li></ul>	<ul style="list-style-type: none"><li>- Very dependent of the design choices made by the bank</li><li>- Reduced performance, due to the fact that a single functionality cannot be called separately</li></ul>
Example	<ul style="list-style-type: none"><li>- Schedule-payment from Bunq</li></ul>	<ul style="list-style-type: none"><li>- PayLah from DBS</li></ul>

Figure 7.

Bank A				
Field	Object type	Description	Example	Optional
id	string	Identifies a reference to a corresponding transaction	"61331236"	optional
account_id	string	Internal account id (not account number)	"91203682"	optional
transaction_type	string	Type of the transaction	"creditcard_payout"	optional
remote_bic	string	BIC / Swift code of bank	"DEUTNL2N"	required
remote_iban	string	International Bank Account Number (IBAN)	"DE89 3704 0044 0532 0130"	required
amount	integer	The amount in account currency, in minor units (e.g., 1 EUR is 100)	12000	optional
currency	string	Currency of Account or Amount. ISO 4217 Alpha-3 - 3 (e.g., EUR)	"EUR"	optional
is_verified	boolean	Indicates whether the transaction is verified or not	Yes	optional
Bank B				
<pre>{   "id": "string"   "transactionType": "string"   "bicCode": "string"   "ibanCode": "string"   "amount": 0   "currency": "string" }</pre>				

Figure 8.

4. Developer Usability

Key messages on Developer Usability:

- Banks must get their Developer registration process right to enable easy onboarding of developers
- Mature open banks add to their Developer Portal's functionality and increase usability by adding tools like app management and comprehensive sandbox features
- New ways of serving developers are being explored, such as offering swagger and postman files and testing API calls with Telegram

Developer Usability refers to the tools, guides and experience provided by the bank to the developer to interact with the available APIs. The usability indicates the ease of use of the portal in general, how effective and efficient developers can find their way around the portal. Developer Usability starts with the onboarding of the developer, the GUI that is presented, the toolset that is being offered and the ability for developers to manage their apps. The range of usability varies greatly where some Developer Portals offer guidance or help by performing any action (e.g. automatic authentication in the sandbox), others introduce new ways to test API calls with Telegram (i.e. BBVA), where other (starting) open banks miss out on these opportunities to interact with developers.

As stated earlier, Open Banking is in an emerging state, this is also being confirmed by the updated benchmark. More banks have launched their Developer Portal but more importantly, several banks have updated their Developer Portal looking for better ways to service and interact with developers and increase the overall Developer Experience.

Various approaches to Developer Usability

The top performing banks, respectively Nordea, ERSTE Group and Fidor, have comprehensive portal usability, app management and sandbox environment. The analysis shows great variance in the offering of a sandbox. The top banks cover the complete API offering in a sandbox and guide developers through the process, having the sandbox integrated and with extended help functionality. Other banks do not offer a sandbox or without a GUI, leaving the developer to only get access to the sandbox through a terminal.

Bunq however, has a deviant approach by offering a large set of useful developer tools and accompanying documentation, including an Android app that connects to a personal test account in the Bunq Sandbox environment. Although this might take some extra time in the initial set-up of the APIs and getting familiar with the Developer Portal, the presence of the available tools (e.g. offering SDK's with the most different (script) languages) seems to make up for it on the long run. Such approach might be a good way of binding with developers, that is, when developers are over the steep learning curve, chances are that they will return to use the respective bank's APIs.

The depth of app management differs substantially across portals from only basic key management functionality to comprehensive management of app permissions, team management (incl. roles) and even app analytics. These are good examples to improve a Developer Portal focussing on how developers are being served by the bank through its Developer Portal. These extended features can offer a big advantage to the developers, especially when third



parties want to offer many different APIs, working with large development teams.

As shown in figure 9, most fluctuation is seen in the offering of SDK's and other developer tools, with Bunq leading in SDK offering and Nordea with additional developer tools. BBVA has the most consistent offering on each category in Developer Usability, by dividing their attention and scoring far above average in each category. Nordea is the clear winner with great Portal Usability and a lot of additional documentation (e.g. many tutorials and guides) to help developers get started.

**First interaction with developers is key**

Additionally, the way the first interaction with developers entering the Developer Portal is shaped, could create a barrier for developers to get engaged. The research shows large differences in 'getting started guides' and 'extended how to's' for developers to get acquainted with the portal and its way of working. Also, for Developer Usability, next to API design, a common set of guidelines for all portals could help developers to get up to speed more quickly. A progressive example would be the Open Banking Project in Nigeria<sup>1</sup>. While this initiative is still in an early stage and mainly focused on API documentation, various elements of Developer Usability are taken into account (e.g. authentication and a sandbox). Creating common guidelines in an early stage for a community of (small) banks in a particular region could contribute to a faster growing ecosystem and increased cross-fertilisation.

**Banks tend to excel in a single capability of Developer Usability**

The data in figure 10 shows that most banks tend to excel in a

single capability of Developer Usability. Nordea, however, is the top performing bank in Developer Usability achieving high scores on two capabilities: 'Registration & Introduction documentation' and 'Sandbox environment'. Nordea's sandbox is intuitive to use and has clear and well-structured documentation. Onboarding is quick and easy with the guidance of their "Developer Portal Starter guide", setting-up an account requires minimal effort. Only two banks (i.e. SEB Group and ING) are offering federated login functionality enabling developers to create their account in just a matter of seconds. Banks, in general, can further improve their Developer Usability by adding 'App entitlement and management' and 'SDK's start-up toolkits' to their Developer Portal.

There seem to be only very few banks (e.g. Fidor, Erste and Capital One) which are focussing on 'App entitlement and management', where a large group of banks offer virtually no related functionality. Considering this is mainly of importance when working with multiple developers on an app, most banks have not met that maturity level on their Developer Portal yet. As stated above this can, however, be a great advantage in serving developers.

The fact that the quality of these capabilities substantially fluctuates across banks emphasises again that Open Banking is in an emerging state. The different capabilities currently being measured will probably be extended in a subsequent release of the OBM. Most likely, the fluctuation of the quality will decrease when Open Banking will achieve a more mature state, leaving fewer different banks reinventing the elements of the Developer Portal as they learn from best practices.

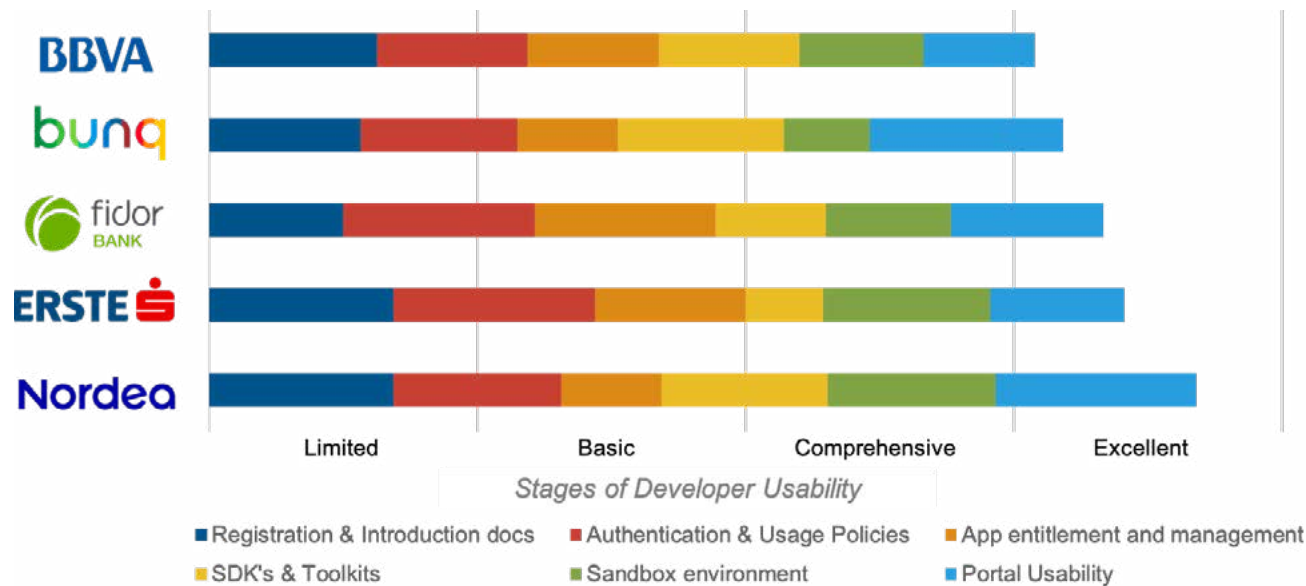


Figure 9.

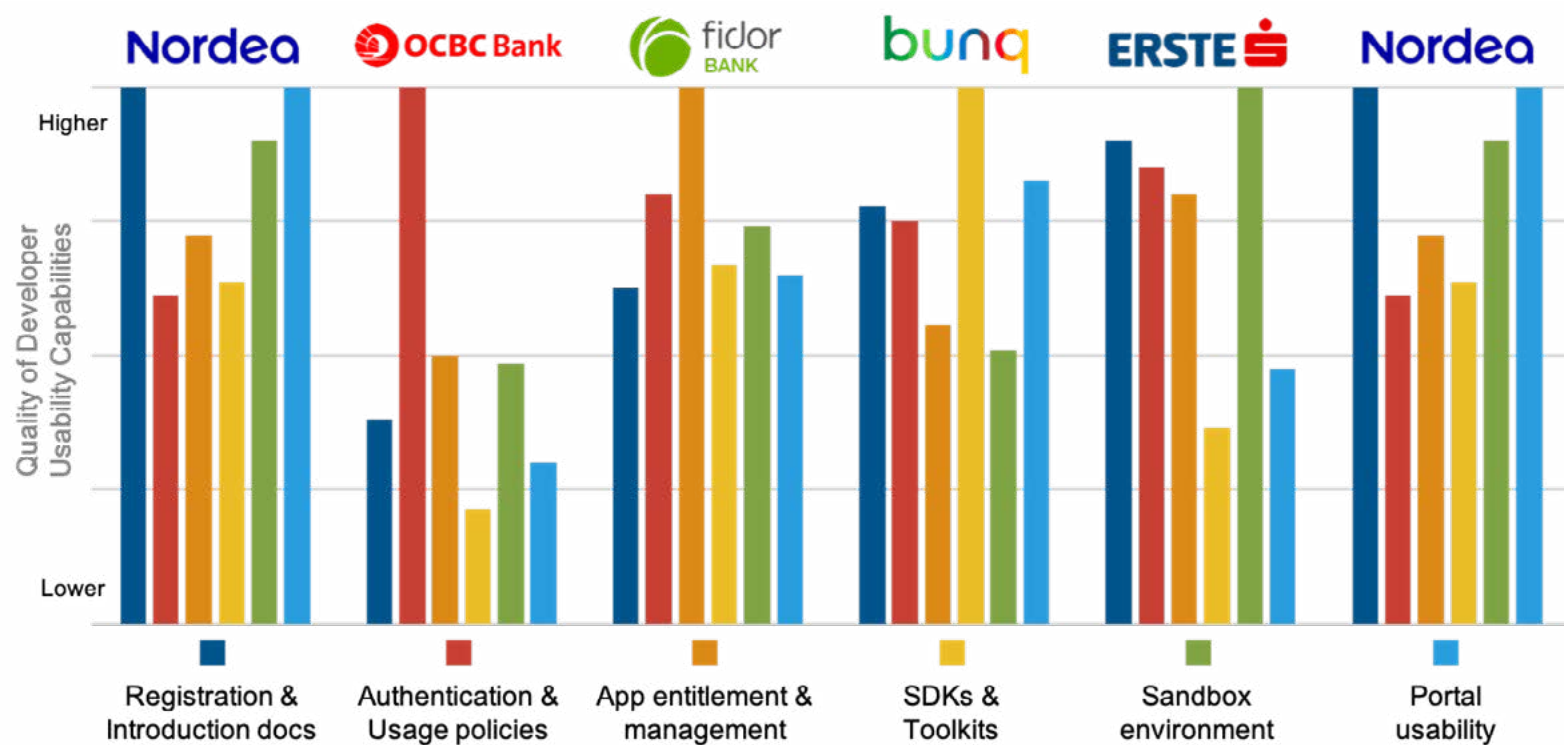


Figure 10.

## 5. Developer Community

Key messages of Developer Community:

- More banks are starting to see the potential of building a Developer Community to strengthen their position as an Open Bank in the ecosystem
- Critical mass is key for enabling a community around an Open Banking ecosystem
- Banks differ in the sophistication of shaping their Developer Community ranging from relatively simple support functions to full-fledged collaboration approaches embedded in other communities

Developer Community refers to the way banks inform actively engage developers to interact with the bank's Developer Portal. Certain banks are actively engaging with developers by creating direct channels to let 3rd party developers get in touch with the bank's developers. Other banks are organising events like hackatons to build and engage the Developer Community.

### Relevance of the Developer Community

The community of developers which is allied to the Developer Portal of the bank can play an important role for the banks position in the Open Banking environment. As the Developer Community increases, most likely production of API consuming apps will also increase. Incentives of developers joining the community might vary from a large customer base the bank is offering, the experience of the Developer Portal, to a functionality which is solely offered by the respective bank. Setting up, maintaining and growing a community around the Developer Portal and/or participating in other's communities

is likely to strengthen the bank's position by encouraging 3rd parties to drive innovation and to offer a greater variety of apps in a faster time period.

### Three stages of Developer Community sophistication

We separate three stages in which the level of community engagement differs with the level of sophistication, respectively 'support', 'manage' and 'collaborate', shown in figure 11.

The 'support' stage can be defined as providing a Developer Portal with a toolset for developers to find their way around. This, over time, will be the smallest investment for the bank,

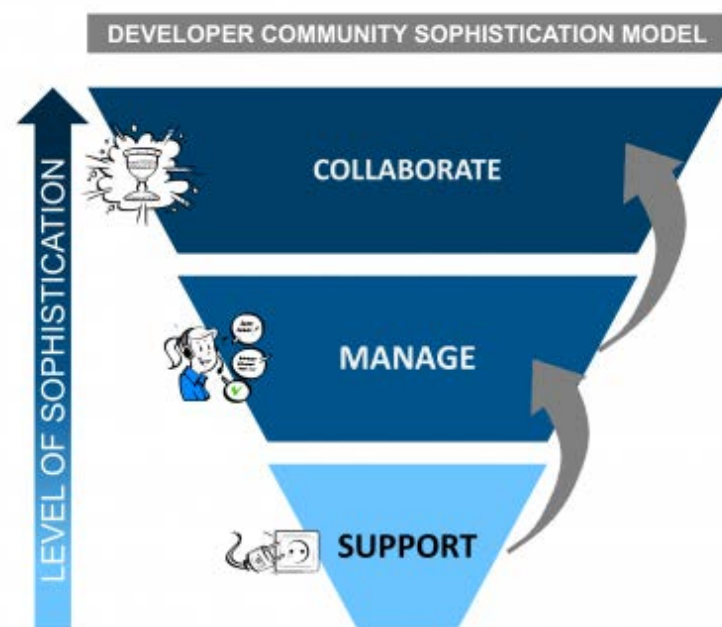


Figure 11.

however this will also have the least effect on growing the size of the developer community and cross-developer collaboration. Examples of banks in this stage would be Standard Chartered, BAML and Lloyds Bank. Most of the banks in this stage are “Starters in Opening-up” gradually working to improve the developer experience of their Developer Portal.

Moving up to the ‘manage’ stage, banks actively provide 3rd parties the ability to get in touch with the banks’ developers, answering questions and establishing online discussions. Guidance through the development process can be actively stimulated by the banks’ developers through dedicated communication channels and messengers (e.g. Slack or Telegram). Offering the ability to subscribe to updates on certain topics or specific APIs will keep developers informed of any changes or new insights in a suitable manner. Getting traction on a more mature level can also involve crowdsourcing idea generation for new APIs and online presence of commonly used forums (e.g. Github or Stack Overflow). Examples of banks in this stage are Swedbank, NAB and Erste Group.

The highest level of sophistication is the ‘collaborate’ stage in which banks actively bind with developers by organising events and hackathons to share experiences and insights. If these events are used adequately, it could lead to strengthening the bank’s position on the Functional Scope of APIs as well as the Developer Experience. Developers can share insights on the usability of the Developer Portal and experiences of the tools can be gathered at first hand. On the same note, new ideas can be generated for an app or a functionality to expose. If these new ideas are used in an updated version of the Developer Portal, developers will feel heard which will increase the likelihood that they will return. This will eventually generate a sustainable community around a banks Developer Portal. Examples of banks

who are actively creating a Developer Community are Nordea, Monzo and Starling.

## 6. Five actions to execute on your Open Banking strategy

With many banks across the globe establishing the basics of their Open Banking API platforms, there is a strong incentive towards differentiation in the emerging Open Banking landscape.

A “one-size fits all approach” will most likely not lead to success, as banks need to make strategic decisions on the four core capabilities, API catalogue, documentation, usability and community. Different types of banks are likely to reap different benefits and experience different drawbacks from engaging in the Open Banking play. Moving forward, it is inevitable, however, that we will witness an explosion of Open Banking APIs.

To support banks in the execution of their Open Banking strategy, we have defined five strategic actions that banks can initiate today, as visualised in figure 12.

**Learn from global API best practices;** Learn from the ‘Masters in Openness’ in the Open Banking Monitor, and from digital players outside the financial services industry. This will provide insight in 1) what APIs other players expose, 2) how these APIs are distributed and potentially monetised and 3) how to create the most compelling developer experience to attract, grow and maintain a strong developer community.

**Develop an API rationale and strategy for your business;** Open Banking in general and API monetisation in particular are definitely not a business model fit for all types of banks. Moving beyond PSD2 compliance APIs, requires solid understanding and decision making on the strategic attractiveness of APIs and organisational and technical readiness to execute. Banks

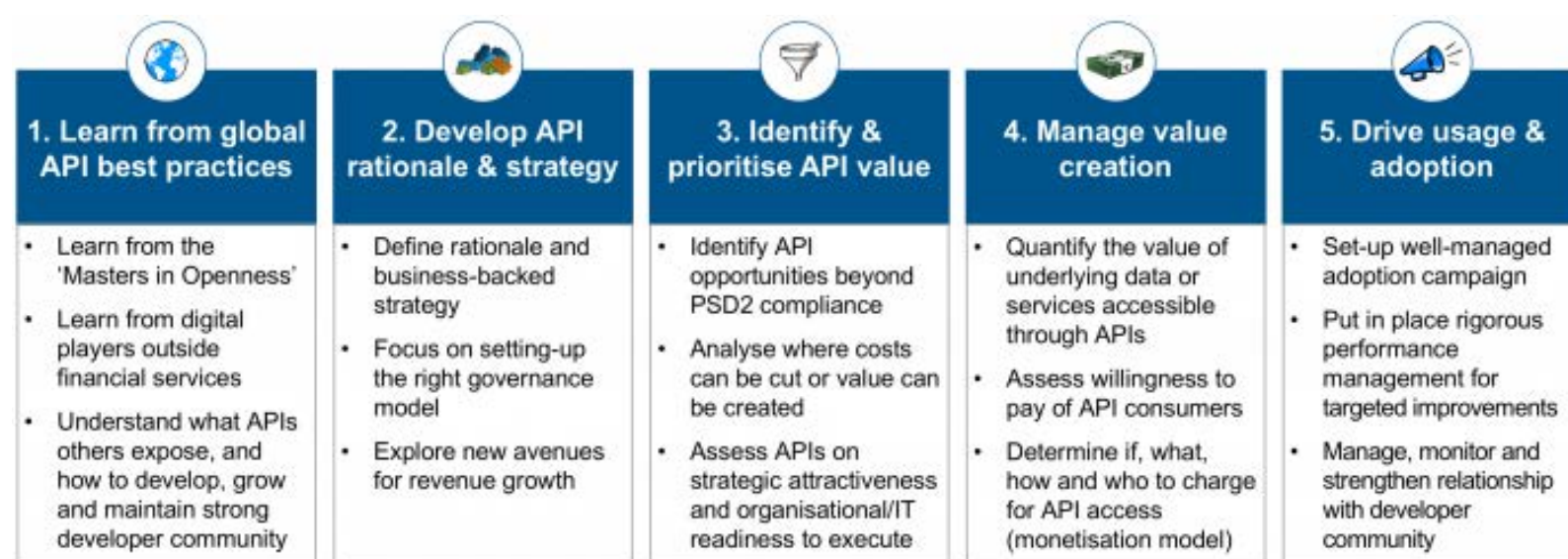


Figure 12.



pursuing an “API first” mentality can generate various benefits both for internal functions and externally, but financial institutions first need to understand if and where best to apply APIs.

It requires deliberate decision making from banks to 1) define a business-backed strategy for different customer segments (e.g. retail, corporate, SMEs, technology players, fintechs), 2) focus on setting up the right governance model to support effective execution of the strategy, and 3) explore ways to create powerful new avenues for revenue growth by assessing if and how potential monetisation models could work in your specific context.

**Identify and prioritise the value that can be captured with APIs;** With a clear strategy in place, banks need to focus on what they need to implement in order to capture the value they have identified. Banks continue their journey by detailing further where 1) value can be created, then they 2) estimate the potential impact in terms of revenue, customer experience, productivity and 3) determine efficiency gains by reducing operational or technology costs through simplified and accelerated development.

**Manage value creation actively;** Banks need to determine if, what, how and whom to charge in a transparent manner. This requires quantifying the value of the underlying data or service that is accessible through an API (e.g. how proprietary is it and what is its role in generating value). In addition, banks need to assess how much API consumers and/or end-users might be willing to pay to access those APIs, to obtain insights in the revenue streams the APIs will open up.

In determining which monetisation approach to use, banks should 1) think about how their data and 2) how APIs can add distinctive value for different customer segments and 3) determine the most appropriate pricing strategy. Those insights can help banks make an informed decision on monetisation arrangements to pursue with different partners and/or end-users.

**Drive usage and adoption to accelerate network effects and gain scale;** Like any product or service, a successful Open Banking API strategy requires a well-managed adoption

campaign backed by rigorous performance management. Generally successful API first approaches start with engagement of selected API consumers and/or end-users to explore what benefits the use of APIs brings. Along the way functional and technical requirements are updated to fix issues, while related business, legal and operational arrangements are put in place to govern relationships. Once this is in place, banks proceed with driving wider-adoption to achieve critical mass among API consumers.

Combined with rigorous, ongoing performance measurement focused on relevant usage and traffic metrics, banks can obtain the needed insights to make targeted improvements and validate desired strategic and customer outcomes. Indeed, delivering innovation through an Open Banking API platform requires banks to build capabilities to 1) manage, 2) monitor and 3) strengthen their relationship with diverse segments of API consumers.

In essence, Open Banking should be approached as a business strategy and business model in its own right, requiring an alternative way of thinking and working in product development. Combined with powerful execution capabilities and a successful and scaled partnership ecosystem banks will be able to future-proof their competitive position in the Open Banking era. INNOPAY’s experience and services portfolio can support banks to design, launch, and scale their Open Banking API platform strategy.



**Author**

Mounaim Cortet, Art Stevens

[ORIGINAL BLOG](#)

[BACK TO INDEX](#)

[SUBSCRIBE FOR NEWSLETTER](#)

PSD2 & OPEN BANKING

# Sharing transaction risk data leads to Open Banking success

Milan Kaihatu, Rob van Meijel  
on October 16<sup>th</sup> 2018



**Milan Kaihatu**  
Senior Consultant

GET IN TOUCH



**Rob van Meijel**  
Consultant

GET IN TOUCH

This article was first published by the Paypers in the [Open Banking Report 2018](#).

The revised Payment Service Directive Regulatory Technical Standards (PSD2 RTS) will come into effect in September 2019. It will require every bank (Account Service Payment Service Provider, ASPSP) to apply Strong Customer Authentication for almost every transaction. Although this increases security, it also introduces unwanted friction in the payment process. Fortunately, there are exemptions where SCA is not required. However, this requires an AS-PSP to perform Transaction Risk Analysis (TRA).

**And therein lies the problem.**

For TRA to be effective, the data about the transaction, the customer and the context needs to be available and analysed, in real-time by the bank (ASPSP). However, with new service providers or Third-Party Providers (TPPs) joining the payment chain, the data is fragmented and distributed across multiple parties. Moreover, although there are several initiatives to standardise the exchange of payment information (through APIs), there is very limited mentioning of standardising context and risk data.

In this article, we elaborate on three key points that need to happen in order for banks to make TRA more effective under PSD2.

## 1. Security and risk data should be shared through open and common APIs.

Security and risk data consist of contextual data that can be gathered during the entire process of the transaction. Collecting data starts when a customer performs a transaction at a TPP. The TPP can read various data points based on the device the customer uses and his behaviour. After that, at the ASPSP, various data points can also be gathered based on attributes of the transaction and of the account.

During this process, the TPP should use the API call to the bank to provide contextual data, which will be assessed within the bank's fraud engine.

This does require parties to use the same protocols and standards for communicating context data.

*Only when the transaction poses a "low level of risk", then the payment service provider is allowed exemption from SCA. PSD2 requires the risk assessment to include:*

- Abnormal transaction behaviour
- Lists of compromised or stolen authentication elements
- Unusual information about the device or software
- Historic transactions of the user
- Amount of transactions
- Location of payer and payee
- Known fraud scenarios
- Signs of malware infection

Multiple standardisation initiatives are aiming to decrease communication complexity between banks and TPPs. In Europe, several initiatives have been launched to create an open and common API standard for PSD2:

- "NextGenPSD2" is the standard developed by the Berlin Group — consisting of almost 40 banks, associations and PSPs from across the EU;
- Also, in Poland (PolishAPI) and France (STET) initiatives were launched by consortia of banks in their respective countries;
- In the UK, the Open Banking Implementation Entity (OBIE) is also working on a common API standard, an initiative mandated by the UK's Competition and Markets Authority in 2016, ahead of PSD2.

However, there is a complication. These standards only marginally discuss the sharing of risk and authentication data. They also differ in their requirements:

- The Berlin Group standard specifies only the IP-address as mandatory (from 1.0 version);
- STET and PolishAPI also add UserAgent as mandatory (information about the device and browser), besides IP-address;
- UK's OBIE refers to the OpenID Foundation Financial-Grade API which prescribes just the "UserAgent" as mandatory;
- The API of OBIE talks about sharing of 'Additional fields identified by the industry as business logic security concerns', but that does not give clarity on which data must be shared mandatorily.

With increased coordination and convergence between different standards, more risk data and authentication data could be added to the APIs. Already, the scope of UK Open Banking has been aligned with PSD2, while STET and the Berlin Group are working together to ensure convergence between standards. Moving forward, these standards could include application and device details, time since credentials change (i.e. change of phone number, e-mail, rebinding of app etc.), time since onboarding of customer.

In addition, aspects of behaviour could also be shared. Think of properties of transactions like the moment of the day when they are usually performed, the receivers and the value of the transactions. Also, through the speed of typing, tilt of the device, and the order of pressed buttons. This behaviour is strongly attached to a device and a person, a combination that is hard to imitate.



In figure 1 a non-exhaustive overview of properties is listed to give insight on what can be used as risk data as input for a risk engine.

## 2. Machine learning becomes the new normal for fraud detection engines.

In open banking, the value chain is less vertically integrated. Without control over the end-to-end process, the AS-PSP needs to be able to gather risk data through additional sources. So, how can banks maintain their ability to detect fraud?

Besides exchanging information with TPPs, banks could also exchange modus operandi (MO) with other banks through an API call. Firstly, this requires banks to develop this capability into their “open” fraud engines so that they can consume external sources of data. Secondly, engines need to be able to analyse and process larger volumes of data in real-time.

For years, rule-based engines have proven to be effective in uncovering fraud for known patterns. However, rule-based processing has an inverse relationship with the size of datasets. By getting input from TPPs and other banks, the amount of risk data grows significantly. Machine learning techniques are faster and more efficient at processing large datasets and can maintain a high level of detection capability while working with large datasets. For discovering unknown fraud patterns out of

large datasets, the application of machine learning is therefore recommended. For machine learning to add value, a large dataset is needed, so it might be worthwhile to start-off with a rule-based engine and then later improve by adding machine learning.

## 3. Use customer involvement as detection mechanism.

In open banking, customers need to have control over their personal data. Without control, customers will be reluctant to share data, or transact with TPPs. Risk engines are able to learn from actions that are initiated by customers. For instance, they are able to detect a security aware customer or a customer that is likely to become malicious. Therefore, giving control to the customer will improve risk-profiling, and therefore transaction risk analysis (TRA) for banks.

A solution that gives the customer a convenient way to manage access to his account would be beneficiary to all parties in open banking. The customer should be able to determine access restrictions for devices and users, and/or provide limits to spending and withdrawals. Based upon the customers’ own insight, he could revoke access, or adapt access requests. Through the same system the customer can also administer which of his own devices are to be trusted, which means that in case of loss he can act upon that immediately.

1. Transaction data			2. Account data		
Time & date	Value of trx	Recipient	Account changes	Time since onboarding	Time since rebinding
Sender	Currency	Transaction ID	Politically exposed	Shared account	Current balance
Occurrence	Description	Merchant ID	Usual login moment	Data combination	Federated access
3. Device data			4. Behavioural data		
Geo-location	Open ports	IP-address	Movement	Tilt of device	Keystroke speed
Multiple devices	Used proxies	Session ID	Keystroke force	Access speed	Gait
User Agent	Application details	Rooted/jailbreak	Sequence of actions	Glitch solving	Eye-movement

Mandated by Berlin Group, STET, PolishAPI

Mandated by STET, PolishAPI and OBIE

Recommended by Berlin Group

Source: INNOPAY analysis (2018)

Figure 1.

### To conclude

It goes without saying that any data sharing initiative should adhere to the applicable privacy laws. GDPR requires a lawful basis for processing personal data. Legal obligation is one of them. The PSD2 RTS on Strong Customer Authentication states in Article 2 that payment service providers shall have transaction monitoring mechanisms in place. Our solution mentions risk data sharing from TPPs towards banks. Part of that risk data is data on behaviour, which is personal data. Therefore, it is important that only the banks risk engine can make use of that data. This can be ensured by using a bank-controlled software development kit (SDK) for gathering behavioural data and sending that data over a secure connection.

Being able to do transaction risk analysis has its benefits for TPPs, banks and customers, but requires ongoing cooperation of the three parties involved. TPPs need to collect and share risk data with banks; banks need to share risk data amongst other banks and delve into the possibilities of machine learning, and customers can contribute by monitoring and controlling the access others have to their data. By combining these perspectives, Open Banking finds layered support aiming to lower risk and set friction to a minimum.

The future will show to which extent transaction risk analysis (TRA) will be adopted for payment services, and a trusted infrastructure will undoubtedly be fundamental to its success.



### Authors

Milan Kaihatu, Rob van Meijel

[ORIGINAL BLOG](#)[BACK TO INDEX](#)[SUBSCRIBE FOR  
NEWSLETTER](#)



PSD2 & OPEN BANKING

# Seamless, Uber-like payments, brought to your bank account

Vincent Jansen on November 27<sup>th</sup> 2018



**Vincent Jansen**  
Partner

[GET IN TOUCH](#)

## **Towards the first pan-European Open Banking based scheme**

**Imagine you're taking an Uber at the airport, get to your destination and while you're getting out of the Prius ... ping... you receive a push notification from your bank that says € 32,78 was debited from your payment account. The full Uber experience, but no cards or wallets needed.**

Maybe, an experience like this is what the EU law makers had in mind when they thought of PSD2 'Access to account' (XS2A). However, one thing we know for sure, under the current regulation and interpretation, this is not what will happen in XS2A practice by default.

Strong Customer Authentication (SCA) requirements prevent a seamless user experience like in this Uber example. A setup like this would require exemptions from the SCA requirements (e.g. whitelisted beneficiary) in order to work.

But exempting SCA - the SCA that was intended as a risk mitigating measure for banks in the first place - comes with... wait for it... yes, additional risk. But additional risk is usually avoided by banks and voluntarily accepting such risk is therefore only done in situations where the benefits outweigh this risk.



Traditionally in payments such benefits take the form of fees the bank collects for the service. On top of those fees, additional risk mitigation is often achieved through a certain liability shift that is contractually agreed upon.

In this example, where Uber would need to be able to initiate payments from the user's current account directly and for variable amounts, without the need for a credit or debit card, there would be a need for a contract between Uber and the bank. This contract would enable Uber to have this feature rich integration with the bank, allowing the typical, seamless, Uber payment flow. The contract would also set fees for this service to be paid by Uber to the bank and would have Uber accept full liability for unjust collections from the user's account.

Now that we know how this setup could work in practice, there's only one hurdle. A hurdle that is not specific to this case by the way, but in fact relevant for almost every meaningful banking service. That hurdle is creating relevant reach to potential users.

Uber is used to working with only a few payment service providers, mostly **Braintree**. Such a payment service provider,

in its turn, is used to working with payment schemes that each unlock millions of potential customers. Without any other arrangement, in our example, Uber or Braintree would need to connect to, and contract thousands of banks before this setup could reach a relevant user base and work on a pan-European scale.

It is for this reason that, in order to make this vision of seamless, Uber-like payments a reality, we need a new scheme. An Open Banking based scheme that offers these harmonised payment services on a pan-European scale and competes with card-schemes on reach, functionality and price.

Now the only question is, what consortium of banks is willing to start making this vision a reality?

Note: since the reach argument is applicable to not only the seamless, Uber-like payments, but to all Open Banking services that operate in a 2-sided market (and a lot of them do), there's probably a need for more Open Banking based schemes to deliver on the promise of Open Banking. We'll explore this in future blogs, so keep posted.



## Author

Vincent Jansen

[ORIGINAL BLOG](#)[BACK TO INDEX](#)[SUBSCRIBE FOR  
NEWSLETTER](#)



OPEN INSURANCE

# Insurance and the Open Banking wave: seven use cases

Maarten Bakker on March 13<sup>th</sup> 2018



**Maarten Bakker**

Director and  
Lead Insurance

[GET IN TOUCH](#)

Every single day, more than a billion active users share their thoughts, photos, news, videos, memes, and more with friends and connections on Facebook. With data from current accounts, bankers know what their customers eat, where they buy their clothes and what they get up to online. In today and tomorrow's world (personal) data is becoming increasingly available and easily shared due to the digitalization of our day to day interactions. New connectivity technology (e.g. APIs) enables consumers and businesses to share more and more data with different parties who again monetize on this data. This frequent and relevant interaction from businesses with their customers forms the basis of new business models in new ecosystems.

To respond to this trend, banks are opening up and create new opportunities for other parties. These new transactional ecosystems focus on gathering data and offer new products and services around these transactions. The payment (functionality) as such becomes less relevant. Insurance companies can capture the new value when they become key actors in this new ecosystem. It is a great opportunity to reshape the current often incidental customer interactions to a more interactive and thus more relevant relationship.



So far, there is no indication that insurance companies are seriously working on the concept of openness. They are at best in an exploratory phase on a new wave of Open Banking data and functionalities. As a consequence, they are falling behind.

### The time is now for insurance companies to move on PSD2 and Open Banking

With the new and much talked about revised European Payment Services Directive (PSD2), regulators aim to boost competition, protect customers and encourage innovation in the digital transactions space. PSD2 is currently in the process of becoming official regulation in member states and introduces various changes. Third party 'access to account' (XS2A) is anticipated most by third party providers (TPP). And even though the anticipated ecosystem revolution promised by PSD2 evangelists is not in sight yet <sup>1</sup>, PSD2 has sparked thinking and implementation on 'Open Banking' to better serve evolving needs of distinct customer segments beyond the regulatory scope.

The first serious steps are taken, and the spark of Open Banking has definitely ignited given the fact that almost all banks are working on exposing additional functionality through their API developer portals <sup>2</sup>. Also, inspired parties are acting on their own and create new interaction modes where customers have access to their account information through a 3rd party app. A good example is the recent announcement by ASN bank, Regiobank and SNS bank where customers can see their account

information of all banks through either one of the bank's apps <sup>3</sup>.

Given the current state of the move to openness by banks, this is the moment for insurance companies to start seizing the opportunities of openness. They should not wait until regulation has crystallized around the current challenges and risk being outcompeted by players who do act.

### How could it look like: use cases for insurance companies

INNOPAY has defined a first set of use cases for insurance companies. The use cases have been mapped on the most important value levers for insurance to capture relevancy and see where exactly the use cases drive value. The mapping is presented in figure 1 and a first description of the cases is given below.

1. **New (cyber)insurance product for a new client segment:** insure TPPs in PSD2 landscape: data sharing through third parties implies new (cyber) risks and thus accountability in case of data breaches. For PSD2 specifically, to be authorized or registered under PSD2, PISPs and AISPs (TPPs) respectively need a professional indemnity insurance or a comparable guarantee. This is mainly needed to cover liability to account servicing payment service providers (e.g. banks) <sup>4</sup>. The first specialists are already entering this market space, like Protean Risk which is underwritten by Lloyd's of London. <sup>5</sup>



Figure 1: Seven use cases in PSD2 and Open Banking for insurance companies, by INNOPAY.



2. **Better deal engines:** PSD2 provides third parties access to payment account information data (AIS). This data can be mined and relevant insights on customer behaviour can be extracted. This behaviour can then be for example spending on insurance to see if a better offer can be made to the customer or looking for patterns which can imply a better risk profile and thus better pricing on insurance products for the customer.
3. **Improve personalised advice:** next to mining, the data can be used to improve personalized advice. Although TPPs are by law only allowed to present the account information of customers, insurance companies can use that information to give advice about their financial situation.
4. **Optimise claims management:** together with other data sources, account information that is shared by customers' banks can be used to create new data sets that could be used to improve reconciliation and reimburse the right amount to customers and gain better insights on possible fraud (by looking at for example customer spending patterns).
5. **Up to date customer records:** although there is no Open Banking standard yet and all banks are developing their own view and strategy on opening up data beyond PSD2 compliance, there are already good examples insurance companies can build upon. For example, banks often have accurate verified address information of their customers. When insurance companies have access to this data, the quality of their customer data records will increase. This will improve conversion ratios when reaching out to customers while at the same time provide a better customer experience.
6. **Expanding service proposition to providing accounts:** with the possibility to execute a transaction (PIS) on behalf of the customer or to check available funds (CAF) the functional scope of PSD2 is limited. But in combination with Open Banking functionality insurance companies can

look for ways to expand their own services by providing account services. Focusing on specific customer needs, customer engagement will increase. For example, insurance companies offering wealth management services can integrate dedicated payment accounts into their products for studying children or elderly care.

7. **Digital identity verification:** banks can help in identifying a person during a digital onboarding or digital identity verification process. This functionality is for example already operated by the banks in The Netherlands under the iDIN scheme.

Before insurance companies move forward and invest in potential use cases they have to ask themselves five strategic questions. Providing clear answers will help them navigating the challenges ahead and make sure their investments are worthwhile.

1. How does openness increase relevance to our customers?
2. Which capabilities do we need to leverage in PSD2 and open banking?
3. How can we partner with the InsurTech scene, which is already developing services around PSD2 and Open Banking, to accelerate?
4. What can we learn from banks and other parties connecting to their ecosystems?
5. How can we attract the right talent to deliver on these new opportunities?

In our [next blogs](#), INNOPAY will further explore the presented innovation opportunities of PSD2 and Open Banking and address how insurance companies can tackle their main questions in this space.

1. Source: <https://www.innopay.com/blog/banks-should-open-up-beyond-psd2-to-deliver-on-the-innovation-promise/>
2. Source: <https://www.innopay.com/blog/innopay-open-banking-monitor-who-are-the-masters-in-openness/>
3. Source: <https://www.nu.nl/apps/5154248/asn-bank-regiobank-en-sns-laten-klanten-rekeningen-samenvoegen-in-app.html>
4. Source: [https://www.vandoorne.com/globalassets/bijlagen-nieuwsberichten/2016/fintech\\_changing\\_psd2\\_regulation.pdf](https://www.vandoorne.com/globalassets/bijlagen-nieuwsberichten/2016/fintech_changing_psd2_regulation.pdf)
5. Source: <https://www.proteanrisk.com/what-we-do/business-insurance-2/psd2-insurance/>

**Author**

Maarten Bakker

[ORIGINAL BLOG](#)

[BACK TO INDEX](#)

[SUBSCRIBE FOR  
NEWSLETTER](#)



## OPEN INSURANCE

# 'Open Insurance': a new mindset for the Insurance sector

Maarten Bakker on March 19<sup>th</sup> 2018



**Maarten Bakker**

Director and  
Lead Insurance

**GET IN TOUCH**

**The Insurance sector evolves at a more leisurely pace than many industries, but according to Maarten Bakker, our INNOPAY Sector Lead Insurance, organisations which are slow to develop open strategies will soon find themselves marginalised.**

We are experiencing exponential growth in the amount of digital transactions and customer data, and this is fundamentally changing how organisations have to do business. Every interaction is becoming a digital transaction and is driving the formation of new digital ecosystems. The direction of travel is predominantly towards greater openness, and the fast-moving Banking sector has grabbed headlines with initiatives such as Open Banking and PSD2. But the trend towards openness is equally relevant to the Insurance sector, where organisations willing to innovate will reap healthy rewards, but those without future-proofed strategies will face critical risks.

### **Openness is essential to secure your future relevance**

Maarten Bakker has been advising the Insurance sector for over ten years, and sees tremendous opportunities for companies willing to revolutionise how they do business.

"The explosion of data transactions will have a huge impact on how insurance companies assess, manage and transfer risks. Smart companies will develop new types of services and deliver broader value propositions for their customers by being present at the life events of their customers. They will improve risk selection by identifying low risk customers,

with shared data from the customer's car, and enhancing the quality of their underwriting processes. They will use data from the customer's connected smoke detector to identify fraudulent claims and improve reimbursement evaluation. And they will be able to tap into new markets by distributing their products through other parties at the point and moment of sale which is relevant for the customer. For example, buying your new home insurance product when your customers are in the process of getting an internet subscription for their new rental apartment."

#### **Failure to innovate will leave companies marginalised**

Innovation within the Insurance sector is currently limited in scope and scale. Maarten says: "Most players are not prepared for the ever expanding wave of data transactions, business models and ecosystems. Innovation is mainly focused on cost-savings and increasing service levels via the digitalisation of existing processes. Where partnerships to form new business models are happening, they are usually closed propositions between a limited number of companies with a specific purpose and thus have only limited reach in terms of new customers or access to new data. The sector is still a long way from mastering the art of developing the type of broad ecosystems which will enable innovation at scale".

Maarten cautions: "The next 18 months will be a real turning point for the sector. Technology companies are moving into this space, and are already changing the landscape. If traditional players do not get their strategies in place quickly, they will be left behind in terms of access to data, new markets and customer interaction points. They will quickly find themselves pushed back through the value chain and marginalised. 'Opening up' takes time – time to develop a strategy and to put the right technology in place – and you can't do this at the last minute."

#### **'Open Insurance' requires a new mindset**

Instead of closed propositions and limited partnerships, the sector needs to follow Banking's example, where rapid transformation is being achieved through a combination of new regulation and adopting the type of mindset which inspired companies like Apple and Google to open up their ecosystems. Maarten believes insurance companies should be focusing in two main directions – utilising more external data from new sources, and sharing of their own data but also their product stack with the rest of the world.

"First, companies should plan how to open themselves up to data from a much broader external ecosystem – sources such as payment transaction data, open banking data, IoT data, and all kinds of social data. Don't think in terms of narrow partnerships with a dedicated IoT supplier and small combined customer base. Look for opportunities to tap into all kinds of open APIs and access data from every step of your customer's journey.

"Second, prepare to open yourself up to 3rd parties. Sharing your customer's data with other players can potentially provide that customer with more comprehensive services. Companies should also think how they can open up their product stack to 3rd parties. Look at how Lemonade is exposing its home insurance product through an API for 3rd party developers, and positioning Lemonade's proposition in whole new ecosystems. This type of approach enables real innovation and will create new business models and revenue streams at scale for insurance companies."

#### **Practical steps to prepare yourself for 'Open Insurance'**

Insurance companies must begin preparing to meet a new set of opportunities and challenges. Successful transition will enable new revenue and business models whilst ensuring continued relevance and growth. Maarten recommends several key steps in this preparation: "Companies should start developing new strategies around open products and the wider eco-systems in which they want to play. They need to open up their platforms and technologies. They need to tackle questions about standards for partnerships and data sharing, and also how to comply with regulation. They also need to consider how initiatives from other sectors could be replicated in the Insurance sector. And they need to think about the new talent they require to facilitate these changes."

We can help companies in the Insurance sector to become part of this new world. We have a long track record of guiding companies to embrace openness through the development of new schemes and standards, and strategies for ecosystems, pricing, technology and regulation. We believe 'Open Insurance' is the future, and we can guide you along this journey.

If you would like to discuss any aspects within this article, feel free to contact Maarten.

**Author**

Maarten Bakker

[ORIGINAL BLOG](#)

[BACK TO INDEX](#)

[SUBSCRIBE FOR  
NEWSLETTER](#)





## OPEN INSURANCE

# How #openness will change insurers' pricing strategies

Maarten Bakker on May 25<sup>th</sup> 2018



**Maarten Bakker**

Director and  
Lead Insurance

[GET IN TOUCH](#)

**“Data, whether it’s location-based or behavior-based data, will help provide solutions, whenever and wherever they occur.” – Brett King, author of breaking banks.**

Although insurers are improving significantly on enhancing the customer experience during onboarding, pricing still seems to be the most important differentiator for customers. Based on INNOPAYs experience with open business models and open architecture in banking and other industries, we believe that consuming APIs in an open ecosystem world is the next step for insurers in offering more personalized and thus better priced products to their customers. Insurers have to (re)set their sights and acknowledge that customer centricity is not about offering integrated propositions but is moving towards many to many solutions in open ecosystems.

The premium a customer has to pay depends for a large part on the risk and thus claims associated with that customer or object which is insured. To stay ahead of competition and to allow for more personalised pricing, insurers need to continuously tap into new data sources which can better predict that risk. There are evident and simple ‘discriminators’ for certain types of claims, for example a working fire alarm to avoid damage due to fire or driven mileage in a car which directly relates to the chances a driver is involved in an accident. Having insight in new data sources for these discriminators during onboarding of a new customer would allow insurers to manage the risk better and offer a more personalised premium to customers.

One new source of insights in these discriminators could be open banking data which INNOPAY explored in a [previous blog](#). Another relatively new and growing source is the IoT market. For 2020, the installed base of Internet of Things devices is forecast to grow to almost 31 billion worldwide <sup>1</sup>. Insurers and InsurTech players (like Neos home insurance in the UK <sup>2</sup>) often in combination with (re)insurance companies, are increasingly developing Internet of Things (IoT) data-based and integrated (end-to-end, including dedicated hardware) insurance solutions but so far success in scaled adoption of these one to one propositions is limited.

These new sources of data for pricing discriminators are increasingly shared in open ecosystems with open APIs. Ecosystems are growing and are predicted to account for \$60 trillion in revenues by 2025, or roughly 30 percent of all global revenues <sup>3</sup>. Open API strategies in these ecosystems thus bring numerous opportunities for companies who want to extend their business model or want to increase the relevance of their product or service for their customers. By opening up, a new network of companies which offer integrated propositions can be created. A well-known example of the latter is the open API of the Philips Hue lamp. When Philips opened up this API, a lot of new services were created by other parties. This made the lamp more valuable for Philips' customers because it had more use cases which lead to more sales and a virtuous circle of growth.

In this open ecosystem world, it is hard to impossible to convince insurance customers to buy into an integrated (end to end) insurance IoT proposition and create a hardware lock-in. This results in a slow adoption rate for the current insurance IoT propositions and again translates to slow and sub-scale new book building and thus shareholder value destruction. Insurers have to (re)set their sights and acknowledge that customer centricity is not about integrated propositions but is moving towards many to many solutions in open ecosystems.

An example of an open ecosystem opportunity in customer's homes is Nest (see Fig. 1), the smart thermostat that learns a customers' schedule using predictive analytics to ensure that the house reaches the desired temperature when coming home. Nest has an open API where insurers, with the customers consent, could tap into to see if they have that working fire alarm (and provide a better priced insurance product).

Insurers are wise to watch out for other open APIs in relevant ecosystems they can consume and start learning. For insurers consuming these new APIs in an open ecosystem allows to gather new data attributes and discriminators, needed to create a personalised customer profile and predict the number and size of claims more accurate. Eventually this will lead to becoming an open insurance company with data integration points in multiple ecosystems (see Fig. 2 on page 57).



Figure 1: Consuming the Nest open API – example for insurers (source: INNOPAY).

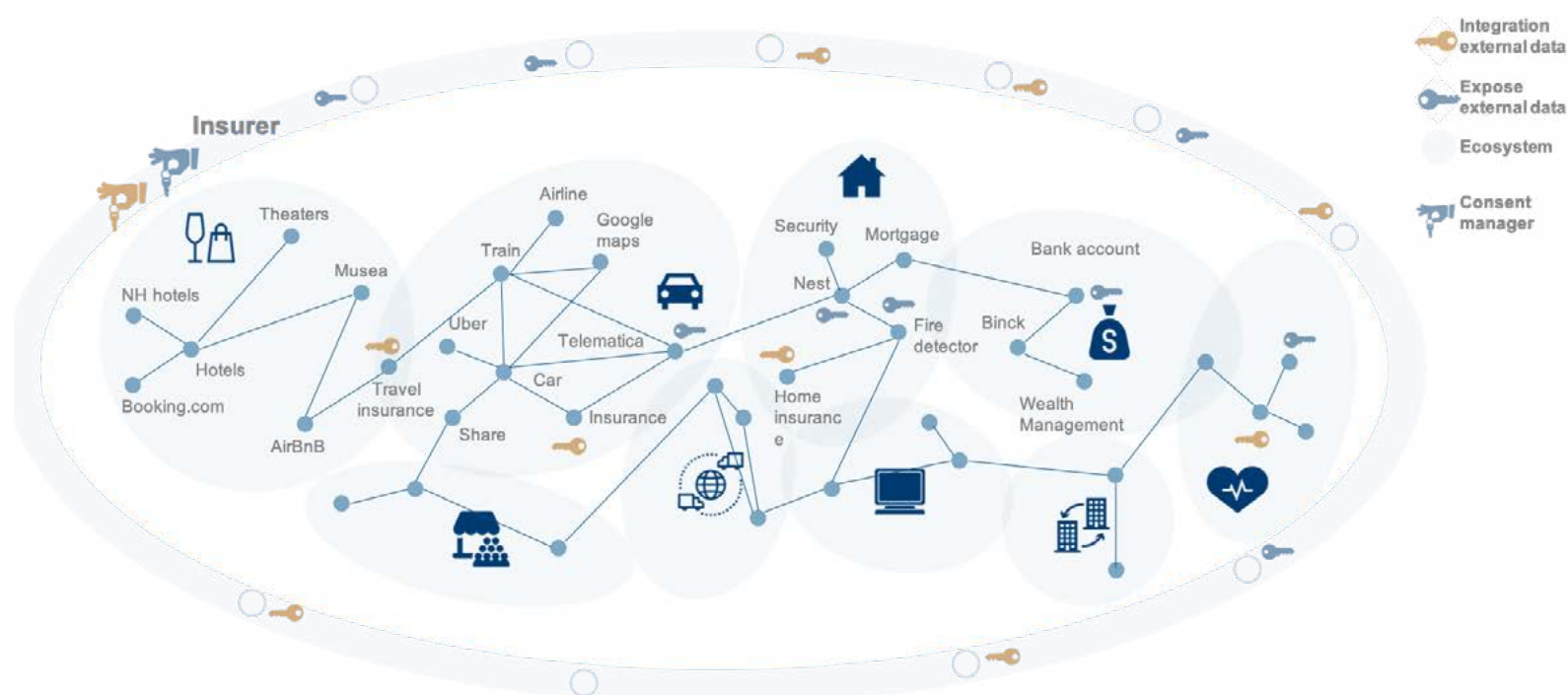


Figure 2: #openinsurance integration in open ecosystems (source: INNOPAY).

There are a number of questions coming into play for insurers when considering to consume APIs in order to increase customer relevance and offer more personalised premiums.

- **API organisation:** consuming open APIs requires a different mindset as value is not developed in house, but sought outside. How to allow for an “outside-in” point of view, providing value to the customer by responding to their needs?
- **Customer experience:** sharing data with their insurer should make life easier for customers. How to allow for a seamless integration of API related questions in the onboarding process and maximise conversion, especially when the insurance is not sold directly? (e.g. via price comparison websites or intermediaries)?
- **Data value balance:** only when customers get something valuable in return they will be willing to share data. How to provide for this balance and convince customers of the added value of these services, in a time where GDPR comes into effect and customers are becoming more privacy sensitive than ever before?
- **Consent management:** in line with GDPR, customers need to provide explicit consent when sharing data. How

to facilitate this in a customer friendly manner and register consent internally in line with regulatory requirements?

- **Data analytics:** when provided access, insurers will gather more relevant data from their customers. How to ensure these are turned into relevant insights and a more personalised offering to the customer?
- **Business model:** developing the capability to consume APIs and offer more personalised services to customers is a competitive asset. How to capitalise on these capabilities and come up with new business models and revenue streams?
- **InsurTech cooperation:** different InsurTechs are already building capabilities for consuming APIs which insurance companies could leverage in their go-to-market strategy. It is important to understand the role they will play in the insurer’s value chain

These considerations show that improved personalized pricing during customer onboarding by consuming open APIs is not an easy thing to do. But it’s a fact that open ecosystems are forming and being present is a must to stay relevant. Based on INNOPAY’s experience with open business models and architectures we know that when done well, the advantages and benefits are endless. Both to the customer as to the insurer.

1. Source: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>
2. Source: <https://neos.co.uk/>
3. Source: <https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/competing-in-a-world-of-sectors-without-borders>

**Author**

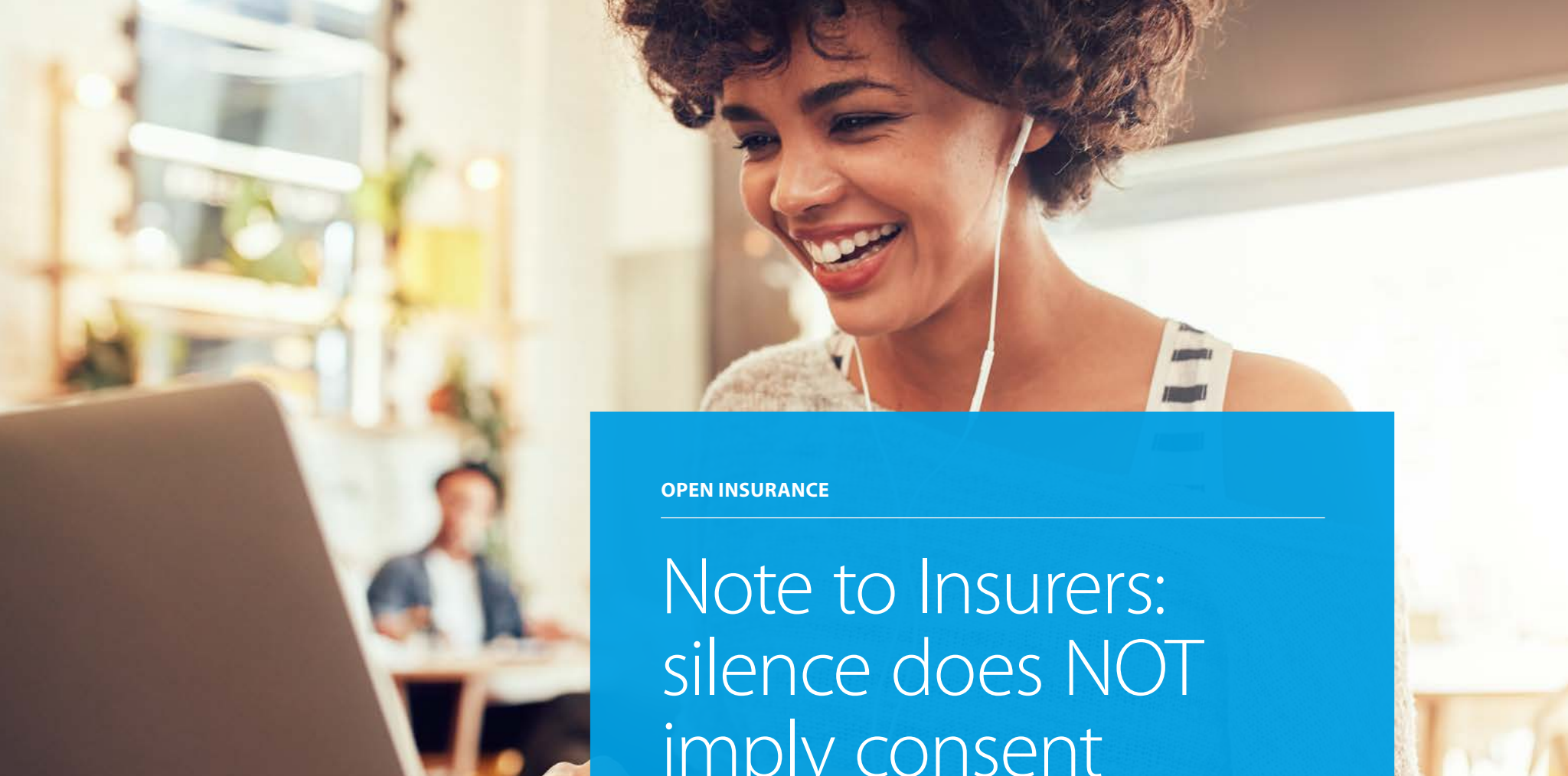
Maarten Bakker

[ORIGINAL BLOG](#)

[BACK TO INDEX](#)

[SUBSCRIBE FOR NEWSLETTER](#)





## OPEN INSURANCE

# Note to Insurers: silence does NOT imply consent

Maarten Bakker, Mathijs Helgers  
on March 28<sup>th</sup> 2018



**Maarten Bakker**

Director and  
Lead Insurance

GET IN TOUCH



**Mathijs Helgers**

Senior Consultant

GET IN TOUCH

**Data and putting the customer in control over his or her data are crucial elements for any platform strategy, especially in an open ecosystem. For insurance companies it means they can extend and improve their service offering and to develop new revenue models. But if they fail to handle the data with sufficient care, they risk damaging the trust consumers place in them. Experts from INNOPAY advise insurance companies to think carefully about their consent infrastructure.**

As society continues to digitalize rapidly and everything becomes a transaction, ever-more data is becoming available that insurance companies can use to their advantage. Access to that data, while being compliant with GDPR, is becoming a crucial element to develop the applications that matter. Among the best-known examples are vehicle telematics devices, which – thanks to the Internet of Things – generate valuable data for providers of car insurance who are keen to gain greater insight into individual driving patterns as the basis for calculating fairer premiums. “But there are many more possibilities, such as fire insurance based on the insurance company having access to the smoke-detector data,” says Maarten Bakker, Senior Manager and Sector Lead Insurance at INNOPAY.

The use of new data sources is already happening. Numerous insurance companies have already attempted to gain insight into consumer driving behaviour by offering to install their own devices in customers' cars, but very few customers agreed to the idea. "That was creating a closed ecosystem, which consumers were wary of. An open ecosystem is actually more interesting because the data from the device is valuable to other third parties too, such as garages that want to be able to notify vehicle owners when maintenance is necessary. An open ecosystem creates opportunities to develop new customer experiences, products and services" explains Mathijs Helgers, Senior Consultant and Knowledge Expert in APIs at INNOPAY. "It's important that consumers retain control over what happens to their data, because they must trust their insurance company that their data won't be sold to third parties," adds Bakker. "Insurance companies need to foster this trust, not suspicion."

### 'Open insurance' - API architectures for new propositions

Today the trend is shifting towards open ecosystems, or 'open insurance' as Bakker calls it. Rather than trying to gather the data themselves, many insurance companies are increasingly making smart use of data generated elsewhere. That is resulting in new risk models, propositions and revenue models, often within new partnerships with organizations that are interested in embedding insurance products in their own propositions. "Data sharing not only enables companies to give better, more personalized advice, but also to offer new embedded insurance products. For example, if you buy a Tesla nowadays, you purchase an embedded car insurance at the same time. The same is happening with the popular VanMoof smart bikes in The Netherlands for which you can purchase an all-in worry-free subscription with insurance, anti-theft protection, access to Bike Hunters and Bike Doctors. These embedded propositions are backed by insurance companies with the use of API based B2B2C platforms and access to the relevant data," states Bakker.

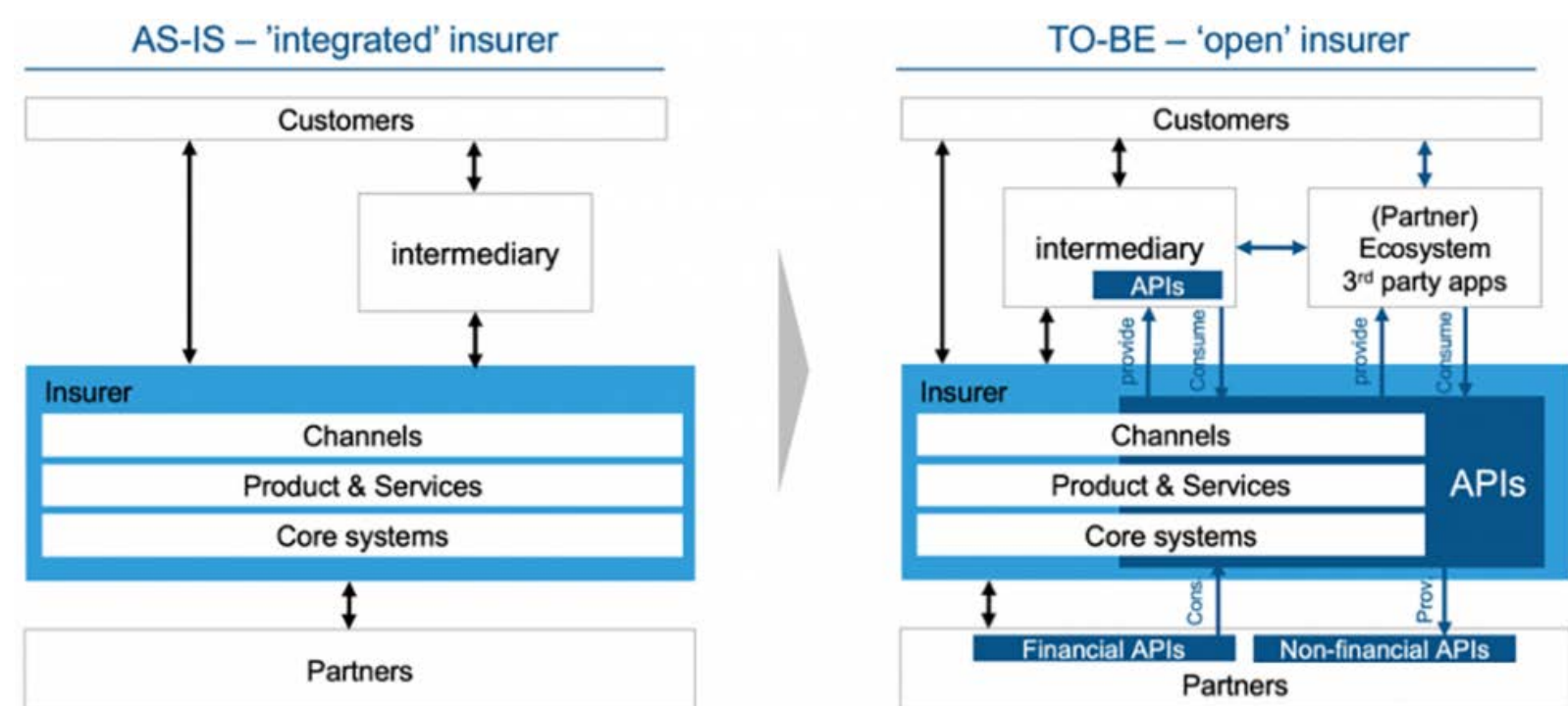


Figure 1: Open Insurer communicates and shares through an API architecture.

Data cannot be shared unrestrictedly, of course. Since the GDPR came into force in spring 2018, insurance companies have been legally required to obtain each consumer's permission for their data to be shared. "But irrespective of the legal requirement, it also makes sense to obtain consent," says Helgers. "For insurance companies in particular, it's important to win consumer trust, and insurers can do that by telling people exactly what information they intend to share, with which partners and why. An effective consent management framework helps insurance companies to position themselves as a trusted partner."

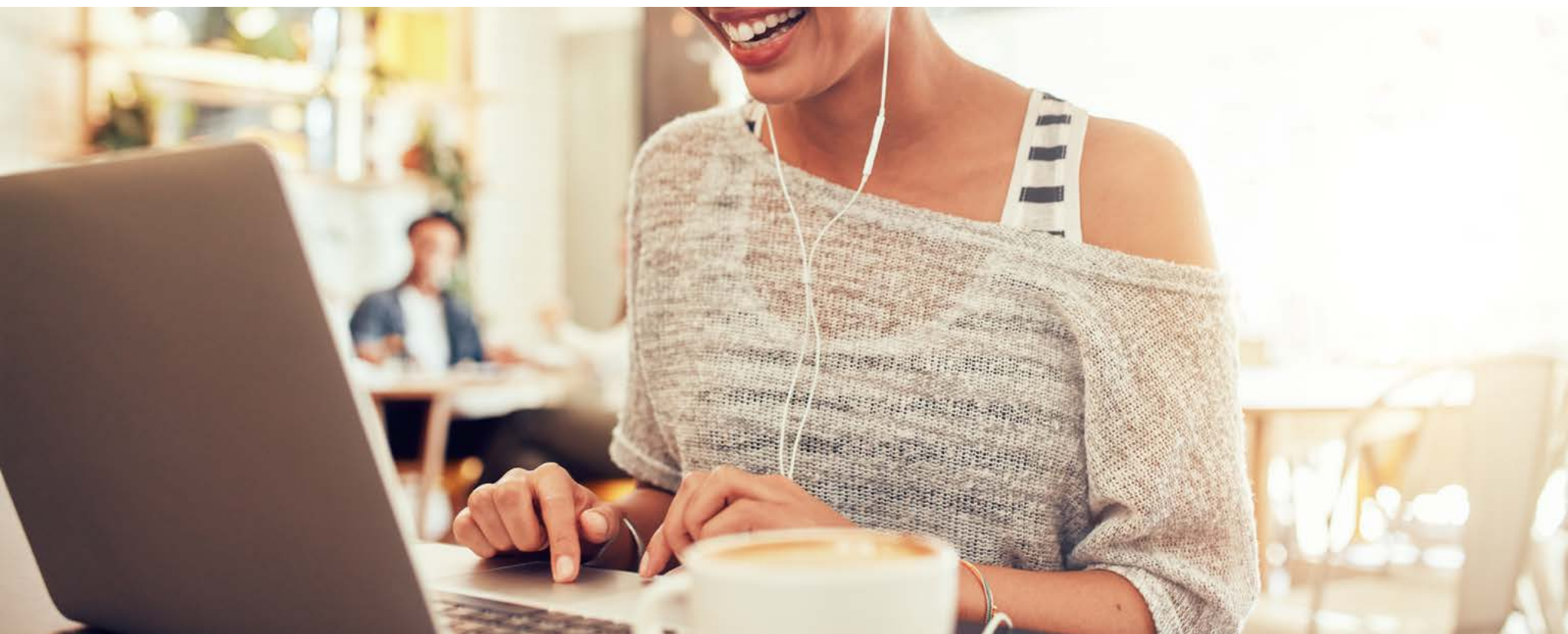
### **Customer in control as the basis for any open platform proposition**

Good consent mechanisms where the customer is in control are especially important in an open ecosystem with numerous parties. It is increasingly common for data in open ecosystems to remain at source. In other words, insurance companies and their partners have to pass through a digital gateway or 'portal' in order to access it, and they can only do so if they have consent. "We are emerging from an era in which companies have been focused on gathering as much data about their customers as possible, but there have also been various scandals related to the misuse of data. Thanks to GDPR consumer data has become

an asset and a liability and it is thus wise to collect no more data than is strictly necessary. If the customer requests a service that requires extra data, the best and only approach is to ask them for consent to use that data," comments Bakker.

Insurance companies are currently working hard to establish new open platform propositions to offer products and services, both of their own and from partners. This requires data to be shared with third parties, but often too little – if any – attention is paid to creating an effective consent mechanism in order to organize the trust aspect of that data. Bakker and Helgers advise those insurance companies to stop and think for a minute. "A consent mechanism for data forms the basis for a platform proposition. Start by formulating your vision. Which role do you, the insurer, want to play in the data sharing? What are the objectives? Which partners do you intend to collaborate with? Which data do you want to share? And how do you plan to monetize it all? Then fulfil that role by ensuring effective consent management which revolves around the consumer."

If you would like to know more about how consent management can support new platform propositions for insurance companies, please contact authors.



## **Authors**

Maarten Bakker, Mathijs Helgers

[ORIGINAL BLOG](#)

[BACK TO INDEX](#)

[SUBSCRIBE FOR  
NEWSLETTER](#)





## ONBOARDING IN FINANCIAL SECTOR

# A pragmatic guide to embracing innovative CDD technologies

Josje Fiolet on April 19<sup>th</sup> 2018



**Josje Fiolet**  
Senior Manager and  
FIn Tech Lead

**GET IN TOUCH**

**Fostering an innovative environment: a pragmatic guide to embracing innovative CDD technologies while effectively managing the associated risks.**

**Financial institutions are investing heavily in technology to improve one of their initial interactions with new customers – the onboarding process. But as they digitally transform their processes, many organisations are struggling to accommodate risk and compliance on the one hand, and customer convenience and innovation on the other. The European Supervision Authorities, supporting new Customer Due Diligence technologies, provide a pragmatic guide for organisations considering how to strike the right balance.**

On 23 January 2018, the European Supervision Authorities (ESA) delivered their **opinion** on the use of innovative solutions by credit and financial institutions in the Customer Due Diligence (CDD) process. The ESAs encourage competent authorities to support digitisation of the CDD process, especially where innovative solutions improve the effectiveness and efficiency of companies' activities for the purposes of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT).

### Fostering innovation through standardisation

The ESAs aim to standardise concrete requirements rather than leaving them open to interpretation by competent authorities and companies, as is common practice today. When these requirements are technology-neutral and promote a risk-based approach, this has the potential to sponsor innovation, especially amongst the more established players which often veer on the side of caution when (re)designing their onboarding and CDD processes. Naturally, CDD processes which are well planned and executed by all players will help to maintain safety and security in the financial sector.

Broadly speaking, innovative solutions for identifying and verifying customers can be grouped into two categories:

- Non-face-to-face verification of customers' identity on the basis of traditional identity documents via mobile devices (commonly used techniques include: video identification, scanning the ID document, or reading the passport by Near-Field Communication).
- Central identity documentation repositories (Know Your Customer utilities which allow customers to store their

data in a single repository that can be accessed by financial institutions for CDD purposes).

When implemented properly, these innovations enable companies to identify and verify customers with convenience, and also to instantly assess the risks associated with a business relationship by reviewing large volumes of data and information from various sources. By automating the identification and verification processes, companies can deploy their staff much more efficiently, and false alerts can be minimised.

### Understanding the risks involved

Organisations should also be aware of the risks and challenges presented by these innovative solutions. It is important that companies can demonstrate to their competent authorities that they have identified, assessed and mitigated all relevant risks before introducing new solutions into their CDD process. Below checklist summarises each factor that needs to be considered: questions which competent authorities should ask (on the left), and guidelines for companies to consider when they supply their answers (on the right).

1. Oversight and control mechanisms When assessing the adequacy of companies' governance and controls frameworks in the context of their decision to use innovative CDD solutions for AML/CFT purposes, the following factors should be considered:		
1.1	Does the innovative solution's design and service offering include appropriate risk management systems that are compatible with products and services offered by companies, especially when the solution is not developed in-house?	Companies should carry out a full assessment of the solution and provide this to the competent authorities on request.
1.2	When outsourcing, do companies retain sufficient decision-making power, specifically in respect of changes proposed to the innovative solution, the onboarding process or the applicable CDD measures?	Companies should have a written arrangement (i.e. service level agreement) in place which details the roles and responsibilities of each party, as well as providing guarantees that the company should be informed about, and have decision-making powers over, any proposed changes.
1.3	Is a process in place that would ensure continuous monitoring of the innovative solution's effectiveness?	Companies should regularly assess the solution and, where weaknesses are triggered, review all affected business relationships and investigate if there is a need for a suspicious transaction report or that relations should be terminated.
1.4	Are controls in place to ensure that companies are meeting their data retention requirements, regardless of the type of innovative solution?	Companies should keep all necessary records that enable them to determine the receipt date and applicable retention period for the documentation, information or data received as part of the CDD process which uses innovative solutions.
1.5	Are controls in place to prevent any data security and privacy breaches?	Companies should be able to demonstrate that they adhere to high standards of data and IT security.
1.6	Have sufficient safeguards been put in place by companies to ensure that the use of innovative solutions does not lead to a breach of data protection legislation or other legislation?	Companies should confirm to their competent authorities that they have examined and assessed the legal implications and have safeguards in place, especially when CDD documentation is gathered in a central repository maintained by an external provider.
1.7	Are sufficient controls in place to ensure that staff conducting the identity verification of customers are not colluding with criminals?	Companies should have controls in place to reduce the risk of collusion through pre-employment screening, random allocation of customers, or screening of employee communications.
1.8	Are sufficient controls in place to ensure that staff using the innovative solution are sufficiently trained?	Companies should provide specific training in addition to general AML/CFT training.
1.9	Are there any compliance and operational risks that should be considered by companies before commencing the use of an innovative solution?	All risks associated with the innovative solution and external provider should be reflected in a risk assessment, and proper contingency plans must be in place to ensure continuity of services.
1.10	Are there laws which do not permit information sharing?	Where companies are unable to meet their AML/CFT obligations because of legal obstacles in third countries where their external providers are located, companies should not engage with such external partners.

Figure 1.

<b>2. Quality and adequacy of CDD measures</b> Article 13(4) of AMLD4 requires companies to demonstrate that the extent of CDD measures is commensurate with the ML/TF risks they have identified. Companies should be able to demonstrate that the innovative solution is reliable. Furthermore, competent authorities should consider the following factors:		
2.1	Are sufficient controls in place to ensure that a business relationship with a customer only commences once all CDD measures commensurate with the ML/TF risks have been applied?	Companies remain responsible and, in the case of higher risk, could consider additional measures. This is especially relevant when identification and verification of customers is performed by external providers.
2.2	Are controls in place to ensure the quality of CDD measures applied and data used or collected, including ongoing and transaction monitoring?	Companies should fully oversee their CDD process on an ongoing basis. Such an oversight framework may include regular assurance testing and ongoing compliance monitoring.
2.3	Are controls in place for ongoing monitoring purposes to ensure that solutions are operating effectively and efficiently?	Companies should consider factors such as the integration of the solution with current workflows, and whether a holistic view of customer profiles can be enabled.
2.4	Are controls in place to ensure that documentation and data gathered remains accurate?	Companies remain responsible for the application of ongoing CDD measures.

<b>3. Reliability of CDD measures</b> Where customers are required to transmit their ID documentation, data or information via video, mobile phone apps or other digital means, companies should consider the following factors:		
3.1	Is there a risk that the customer's image visible on the screen is being tampered with during the transmission?	Companies should have sufficiently robust controls in place to prevent or reduce these risks, and should consider a number of factors such as live chat or other built-in digital applications.
3.2	Is there a risk that an ID document displayed on the screen belongs to a similar-looking person?	Companies should have built-in features that can identify discrepancies, or sufficiently trained staff who are responsible for doing this.
3.3	Are controls in place to ensure that identity documents produced during transmission have not been altered or recycled?	Companies should reduce the risk of these breaches by using built-in security features within the document, limiting the acceptable identity documents, or using a qualified electronic signature.
3.4	Are controls in place to ensure that most potentially suspicious transactions have been identified?	Companies should gauge the quality of outputs and alerts by comparing the outcomes of innovative solutions with their existing solutions.
3.5	Where solutions are used to assess ML/TF risks associated with a business relationship, is all available data and information used in this process and is it considered reliable?	Companies should use multiple reliable and independent sources to create a holistic view of the customer, e.g. online news and publications, social media and public databases.

<b>4. Delivery channel risks</b> There is an expectation that companies carry out an assessment of ML/TF risks associated with non-face-to-face business relationships and the extent to which the use of innovative solutions can address those risks. The following factors should be considered by companies:		
4.1	Is there a risk that potential customers could be impersonating another person?	Companies should be able to demonstrate to their competent authorities that they have assessed the availability and effectiveness of safeguards that could mitigate these risks, e.g. via verification of the identity on the basis of a notified e-scheme (as defined in EU No 910/2014), where scheme's assurance level is high or a combination of checks
4.2	Is there a risk that a customer could be intimidated during transmission of identity verification?	Companies should have strong controls in place to identify possible coercion, which may include a built-in technical feature whereby a customer is required to have a live chat with an administrator who is well-trained to spot abnormalities.

<b>5. Geographical risks</b> Customers are no longer required to live in close proximity to companies whose services they intend to use, and do not need to be physically present for identification purposes. Companies must remain mindful of the risk that a customer may be looking to access financial services in another member state for ML/TF purposes. Competent authorities should consider:		
5.1	Are companies able to assess geographical risks, including having controls in place that capture their customers' location (device fingerprinting or GPS data on mobile phones to establish jurisdiction associated with higher ML/TF risk).	Companies must remain mindful of the risk that a customer may be looking to access financial services in another member state for ML/TF purposes.
5.2	Do companies have practices in place to assess the reasons why customers from other jurisdictions are using their services.	

Figure 2.



By using these guidelines, financial institutions can more easily embrace digital opportunities, and quantify the risks and security aspects of using innovative solutions. It is no longer a question of whether to provide services online, but only how to do it in an effective way. Each question on the checklist should serve as input when considering new solutions and performing a risk assessment. Which is common practice anyway. The answers on the right should serve as guidelines. The ESAs should remain technology-neutral; there are multiple technologies that can be fit-for-purpose, all depending on the risk profile of the organisation, the type of service and the prospect or customer involved. CDD processes should rely on a sensible combination of multiple technologies and mitigating measures.

#### **Working with solution providers to foster innovation in a controlled way**

Technology solutions and their providers should always fit the organisational context. At INNOPAY we believe that successful onboarding processes are modular. For each 'building block' in the process, suitable specialised solution providers can be integrated. The most successful companies are not those which build the entire solution themselves, but those which offer a seamless onboarding experience by connecting the right technologies and providers throughout the chain.

Redesigning onboarding and CDD processes are one of the challenges of the digital transformation journey. Our advice would therefore be to first try the solution within a smaller context, for example with one specific product or customer segment that is considered a low-risk category. This might be contradictory to one requirement referred to by the ESAs under 'Quality and Adequacy of CDD measures,' whereby the 'new solution should be integrated with all existing workflows and legacy systems'. To enable quick and agile development, financial institutions sometimes have to put aside all current processes and go around them. It's an ideal situation to aim for an holistic customer perspective, but in reality, it's difficult to achieve in the beginning. The Digital Transformation journey requires a step by step approach.

Nevertheless, we welcome the ESAs' acknowledgement that third parties can be used for CDD purposes as long as organisations consider the associated risks and mitigate them properly. The ESAs also encourage competent authorities to engage with specialised solution providers and the companies which want to use them, to discuss the impact of these solutions. Greater knowledge and understanding will foster an innovative environment that improves both the security and the convenience of CDD solutions – and this can only be a positive development.

If you are considering how to improve your customer onboarding or related CDD processes, feel free to contact us.



#### **Author**

Josje Fiolet

[ORIGINAL BLOG](#)

[BACK TO INDEX](#)

[SUBSCRIBE FOR  
NEWSLETTER](#)



ONBOARDING IN FINANCIAL SECTOR

# The battle is ON: incumbent banks accelerate onboarding innovations

Josje Fiolet, Jim de Wolf, Jurriaan Wesselink  
on July 12<sup>th</sup> 2018



**Josje Fiolet**  
Senior Manager and  
FIn Tech Lead

[GET IN TOUCH](#)

**Where newer and smaller banks used to outclass the incumbent banks regarding the onboarding process, the recent INNOPAY benchmark shows a comeback of the established players. By now, there is no longer a need to visit the office to open an account. Now the question is: did the larger banks manage to compete with the challengers?**

Our previous onboarding benchmark releases show that in a 6-month period of time hardly any improvements occurred in the onboarding processes of the larger banks. In the fast digitizing world where banks increasingly have to compete for the customer relation, it was surprising to see that so little changes were made in the first interaction with the customer by these players and that the need to visit an office remained.

One logical explanation for the larger banks to have been hesitant towards the use of online identification techniques is that they often find themselves in a split between balancing risk and convenience. They have a different risk profile and a bigger impact on the financial sector as the challenger banks do and as such compliance requirements dominate these discussions in most cases. But then the question becomes if banks will ever be able to offer the same seamless user experience and compete with the challenger banks. This blog intends to answer exactly that question.



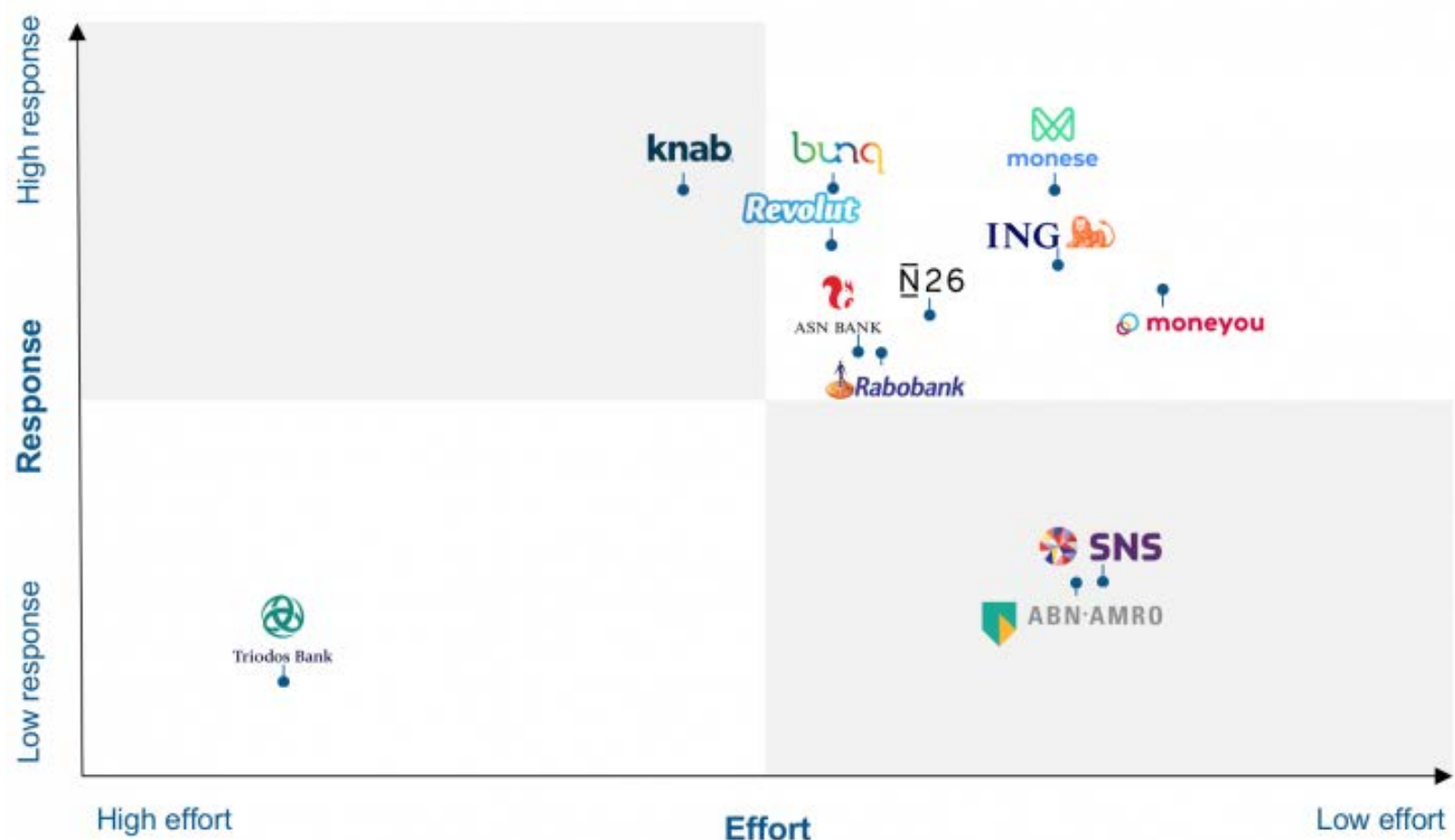


Figure 1: INNOPAY Benchmark of the Dutch market, Q2 2018.

### Big banks on the move

With the Q1 benchmark publication it was already mentioned that Rabobank introduced their full online process for current customers turning 18. Now also ING and ABN AMRO Bank introduced their fully online processes, but for new customers. The changes led to a dramatic shift of ING and ABN AMRO Bank from the left side of the matrix to the right. As the benchmark shows relative scores, all parties shifted in position. So, what was it that stood out?

### Different approaches, different user experience?

With ING it is now possible to become a verified customer within approximately 15 to 20 minutes. For identification, ING uses a similar process as Rabobank does; an NFC scan of the passport and a selfie with flashing light technology to detect if a photo or screen image is being presented instead of a real face. The colour technique is considered to be an improvement in available techniques and is relatively new. That, combined with the fact that the NFC read is only available for Android could have been a reason it took ING a bit longer to release their online process.

ABN AMRO Bank took another approach. For identification they use similar techniques as the challenger banks do, and they are also the first Dutch bank to fully remove the iDEAL payment from their process. And it has to be admitted that they are right to do so. There's no real value in the derived identification method with all banks using it. Pretty soon it becomes 'the derived of

the derived'. Before, iDEAL could also be seen as proof the person was living in the Netherlands (often a requirement when opening an account), but with for example Bunq allowing to open an account as a non-inhabitant, this is no longer the case. If banks would still like to use derived identification to mitigate their risks, they could better use iDIN<sup>1</sup> that provides for verified attributes.

With authentication ABN AMRO Bank remains on the safe side, with them providing hardware in the form of an e.dentifier. The customer needs this e.dentifier to activate the app and for authentication purposes this provides for 'something you have' and 'something you know'. Opposed to an app, for authentication the chip of the debit card can be used and as such the use of the e.dentifier and the debit card for authentication is by some considered to be more secure than the app combined with a PIN. Reasoning from a convenience perspective however, ING has an advantage that everything can be done in the app and no physical hardware is required. As hardware needs to be sent by postal mail this imposes waiting time. ABN AMRO could consider to reduce this friction, by activating the app during the online identification process and allow customer to make transactions right away. This would significantly increase the response score. After all, right after online identification, there is no need for further assurance during that session. Of course, in case of re-activating the app, the e.dentifier, debitcard and pincode can be used.



Something that is not included in the scoring, but is interesting to have a look at, is how the larger players approach the tone of voice and branding in their new processes. Larger banks have a tradeoff between servicing the current (broad) client portfolio or focusing on a specific target group. Balancing these interests is complex. Challenger banks such as Moneyou and Monese are mainly focused on millennials and their digital onboarding process have this distinct ‘millennial’ flavour to it. ING and ABN AMRO also seem to focus more on the ‘younger’ and tech-savvy audience, exemplified by employing more informal text, using slick interfaces and bright and flashy colours. Potential waiting time is made fun and is restricted to a bare minimum.

### Balancing risk and convenience

As the benchmark only takes the customer facing process into account, it is hard to conclude how the banks are able to balance risk and convenience. What can be analysed are the means of identification or verification they use, and to what extent this differs between the larger and smaller players.

As figure 2 displays, both incumbent and challenger banks demand verification by 2 to 4 verification methods. The most frequently used combination is the scan of the ID document combined with the selfie and a payment. Within different methods, there are multiple technologies to use. The flashing colour selfie technique can be considered a more reliable solution to guard against spoofing attacks than for instance a selfie where the person has to blink the eyes. The same goes for scanning the document; with NFC it is actually proofed the person is in possession of the document, where with a photo this could still be a copy of the document. ASN Bank, Knab and Triodos only request a copy ID, which from a security perspective can’t be compared to the techniques used by other players.

Based on these results the impression arises that searching for the right balance between risk and convenience does not necessarily hamper the creation of a competitive onboarding process. As techniques evolve, processes can become more and more secure, while also providing an excellent customer experience. It’s time to realise that risk and convenience are no longer opposites and can be approached as two sides of the same coin.



Figure 2.

### Bridging the gap

Altogether, we have seen remarkable changes in the benchmark over the last three months, with finally the big banks making their move. They come close to bridging the gap with the challenger banks. As it seems that many onboarding features that were once considered as standing out now become more mainstream, new standards on what is competitive arise. We encourage this strive to perfection. To reflect these new tendencies our next benchmark will take into account new and more aspects on what makes an onboarding process outstanding. Stay tuned!

### About the INNOPAY Onboarding Benchmark

INNOPAY is dedicated in helping clients to embrace the opportunities of the digital ecosystem. Onboarding is the first interaction of the organisation with the client and an important enabler to establish trust. Through our Onboarding Benchmark we provide organisations exceptional insight into how their onboarding processes compare to other organisations in the financial services sector, reasoning from a customer perspective. Every quarter we update the benchmark, allowing banks to learn from each other and to ensure that onboarding remains a topic on the agenda. For more information on the benchmark, we invite you to contact us, or to visit our [website](#).

1. iDIN is a Dutch identification service developed by the Dutch banks. It works similar as iDEAL with the main difference that verified attributes are provided. For some banks iDEAL is still preferred in the onboarding process as it also provides the bank account number of the user.



### Authors

Josje Fiolet, Jim de Wolf,  
Juriaan Wesselink,

[ORIGINAL BLOG](#)[BACK TO INDEX](#)[SUBSCRIBE FOR  
NEWSLETTER](#)



## ONBOARDING IN FINANCIAL SECTOR

# How banks can solve the “Onboarding Puzzle” in the German market

Joris Eckrich, Tian Eckrich on June 24<sup>th</sup> 2018



**Joris Eckrich**  
Senior Consultant and  
Onboarding Lead  
Germany

[GET IN TOUCH](#)



**Tian Genthner**  
Business Analyst

[GET IN TOUCH](#)

**In the past few years new and innovative banks, also known as challenger banks, have entered the scene to disrupt the German consumer banking market. Even though a customer does normally not sign up for a new bank account every year, those new players have been recognised to attract and convert a rapidly growing digitally-savvy customer base. While many incumbent banks are still struggling to orient themselves in the digital age, challenger banks have embraced new technologies to optimise customer-centric journeys, having built digital propositions from scratch.**

INNOPY developed a Benchmark that provides banks with essential insights into how to make a good first impression on customers. The first research focused on the Dutch retail banking market, where over the last year all banks made it possible to digitally open a payment account, using innovative solutions. Based on the expertise gained from the Dutch series, INNOPY has enhanced its Benchmark model to reflect the progress observed and to account for the characteristics of the German market.

Our latest Benchmark, completed in Q3 2018, provides executives with an overview of their bank's position within the competitive landscape and product managers or product owners with key learnings on how to improve the onboarding process based on best practice in the German market.



Six key actions have been identified that banks should execute in order to provide the prospective customers the best-possible onboarding experience and increase conversion rates.

1. Eliminate all channel breaks to enable an end-to-end fully digital onboarding experience.
2. Make required onboarding information and prerequisites transparent and understandable for the customer.
3. Guide the customer through the onboarding flow and empower customer support to help prospects during onboarding in a quick and high-quality manner.
4. Make use of tools that ease the process of data entry and eliminate errors.
5. Enable customers to instantly login and start using the payment account after a successful onboarding.
6. Deliver a consistent look and feel throughout the whole onboarding experience.

### Find the sweet-spot within customer onboarding

Not only is the onboarding process for many customers the first interaction with a bank, it is also transpiring the mission and strategy for an organisation and is key for any bank's conversion rates. It is challenging for organisations to find the optimal way of offering their services online; they need to balance security, compliance and risk, while keeping a seamless user experience. Therefore, in order to optimise the onboarding process, the bank must find the right balance among (1) customer capabilities & preferences (2) organisational capabilities & preferences and (3)

regulatory & risk requirements as shown in figure 1.

### Challenger banks are ahead followed by two large incumbent banks

The INNOPAY Digital Customer Onboarding Benchmark shows that challenger banks such as N26, Yomo and Fidor are leading the pack, closely followed by the German 'flagship' universal banks Deutsche Bank and Commerzbank. The Benchmark takes the specifics of the German banking market into account. Due to high fragmentation the results will be presented in four clusters: challenger, direct, cooperative & savings and universal banks.

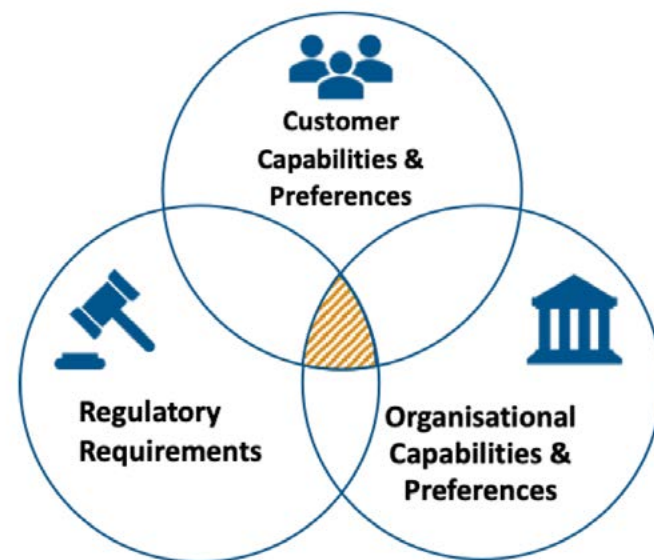


Figure 1: Finding the sweet-spot of the digital onboarding experience

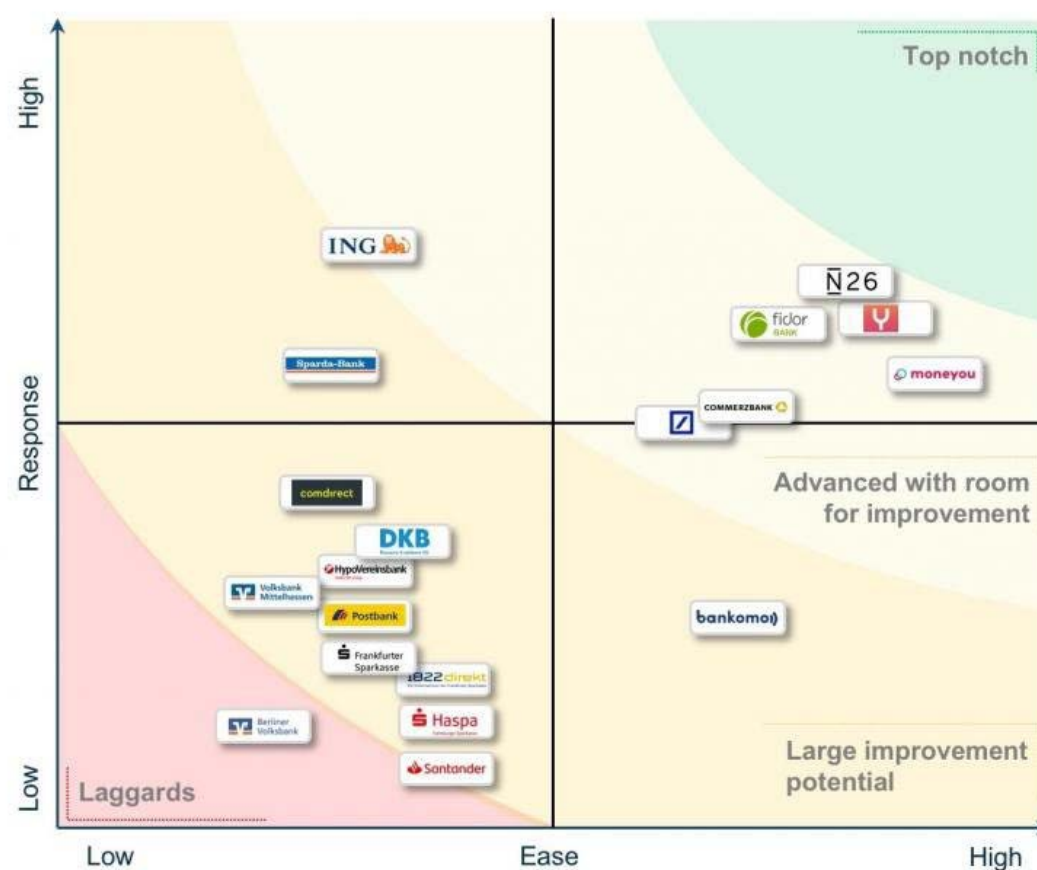


Figure 2: Results of the INNOPAY Digital Customer Onboarding Benchmark Germany (Q3 2018) / Source: INNOPAY analysis

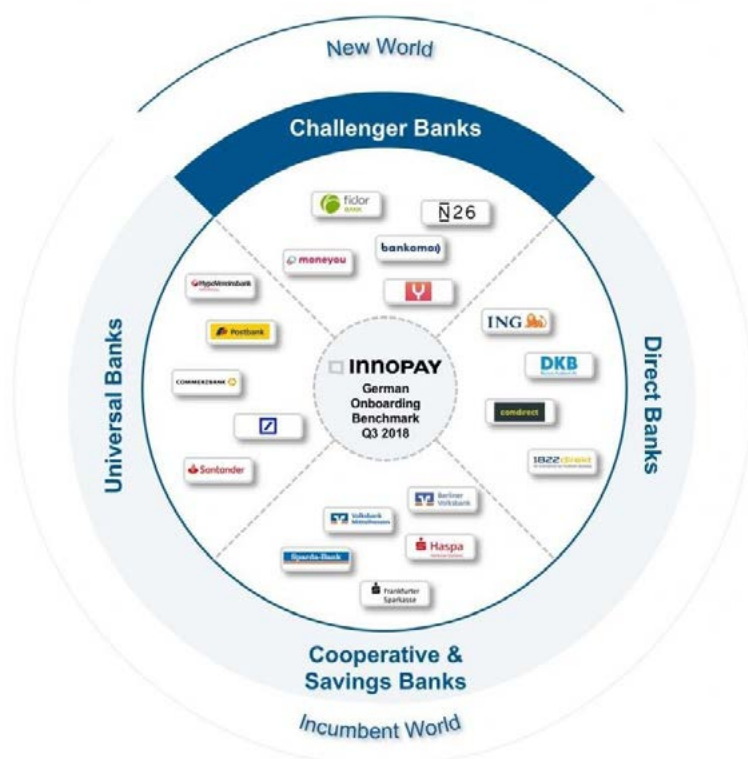


Figure 3: Researched banks for the INNOPAY Digital Customer Onboarding Benchmark Germany / Source: INNOPAY analysis

### Challenger banks are leading the digital onboarding best practice within the German market

Most of the institutions in the challenger bank cluster are located in the upper right range and are thus leading the best practice in the German market. Challenger banks have mostly built their digital proposition from scratch using the latest technologies and could therefore gain a competitive advantage. Their onboarding processes offer a fast, seamless and convenient digital onboarding experience for their customers. Especially the ability of the customer to select the login credentials during the account opening process creates a faster and more seamless experience that is covered well by the challenger banks. Researched challenger banks represent the highest scoring within the four defined clusters. However, none of the banks in this cluster has reached a top-notch position in the Benchmark,

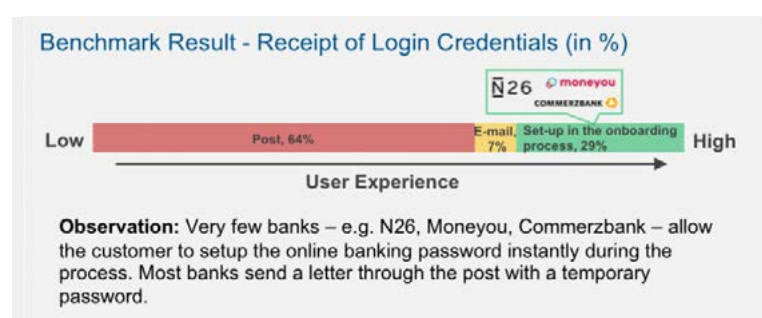


Figure 4: Extract of detailed results from the INNOPAY Digital Customer Onboarding Germany Report – Example from the ease-axis for the receipt of the log in credentials / Source: INNOPAY analysis

thereby every single participant can still improve. Even though many challenger banks are offering strong and customer-centric processes, some are still lacking transparency on the requested data and the key ability to deliver instant feedback<sup>1</sup> on the successful completion of the onboarding process.

### Direct banks need to speed up the velocity of customer onboarding

Most of the direct banks offer a transparent account opening process, in the sense that all required information is shown to the user upfront and the required fields are explained well. Furthermore the direct banks offer a high degree of flexibility and guidance, where the average amount of offered support channels stands out. Not so long ago, “direct banks” were seen as the innovators, challenging established market actors. However, the results show they have been surpassed by new challenger banks. The direct banks are positioned higher than the average scoring across banks but are still behind on using their full onboarding potential. Direct banks should focus on improving the ease of the onboarding process to increase conversion. In some cases, a fully digitised process is present with instant feedback, nonetheless, multiple channel breaks<sup>2</sup> exist that negatively affect the scoring. These channel breaks, potentially

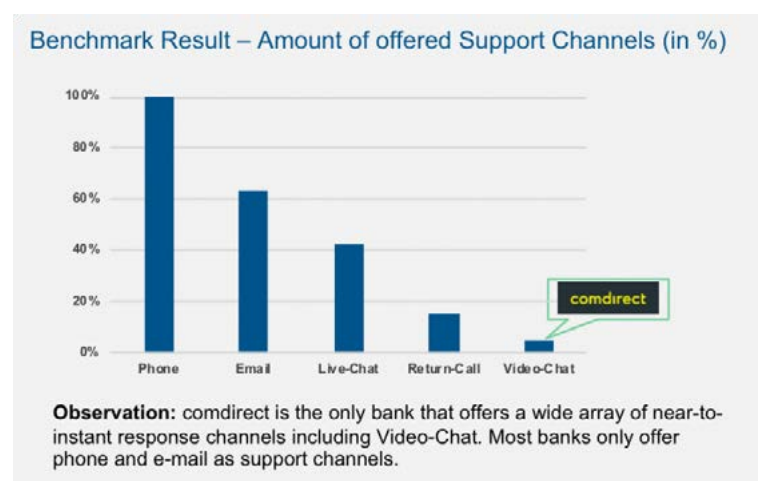


Figure 5: Extract of detailed results from the INNOPAY Digital Customer Onboarding Benchmark Germany Report – Example from the response-axis for available support channels / Source: INNOPAY analysis

caused by legacy systems, are severe as they contradict to offer a seamless and consistent process. This demonstrates an opportunity of improvement where the process is fully digitised and the account is instantly useable.

### Universal banks show scattered results, while the larger banks are leading

The Benchmark shows a large dispersion within the cluster of universal banks, where generally larger universal banks are better positioned than smaller ones. The dispersion can be explained by (i) the broad definition of the chosen cluster

labelling and (ii) different capabilities of process optimisation among universal banks. Larger universal banks might be able to allocate more resources to the adaption to new trends and technologies which are promoted by frontrunning performers in the Benchmark. They position themselves ahead of their smaller counterparts and closer to top performers by having more digitised and customer centric onboarding processes. Smaller universal banks mainly position themselves in the area of large improvement potential, still relying on the classical onboarding approach at their branches, regardless of having a digital onboarding process. In opposition to larger banks, a lack of knowledge was observed regarding the digital onboarding process among customer support representatives of smaller banks<sup>3</sup>. Larger banks have proven that 'incumbent' does not mean 'old-fashioned' and that smaller banks can learn from their larger counterparts.

### **Cooperative banks and savings banks score lowest and have the highest potential to improve the digital onboarding experience**

The sample of cooperative banks and savings banks shows a lot of room for improvement for this cluster. They are primarily positioned as laggards in digital onboarding and have large improvement potential in all relevant areas investigated. Most cooperative and savings banks have similar defining scoring factors on which they can improve such as instant feedback, receipt of login credentials and customer support. For a majority of cooperative and saving banks the look and feel of the digital onboarding experience clearly lags behind its competitors from other clusters. This might be explained through a still prevalent focus on the branch experience within this cluster. Nevertheless, new 'in-house challenger banks' may allow cooperative and savings banks to catch up with the competition in the nearby future. Even though those banks are clearly lacking behind, openness for improvement may enable them to regain a higher position in the future.

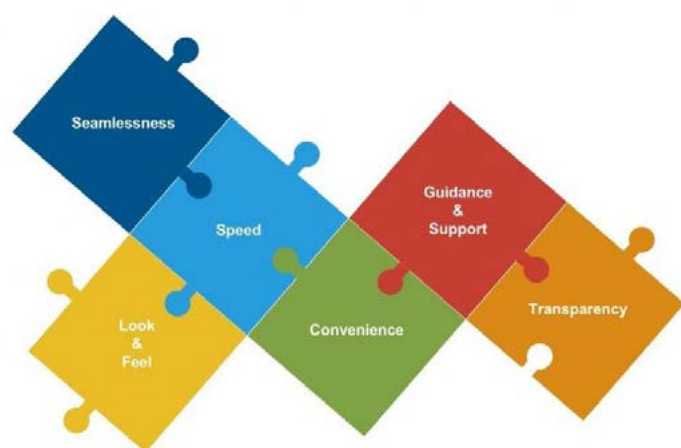


Figure 6: 6 main components solving the puzzle for a successful digital onboarding experience / Source: INNOPAY analysis

### **Key recommendations to solve the onboarding puzzle and to create a great customer experience from the first moment**

Although the four analysed clusters show a diverse range of results, INNOPAY has identified six general components and formulated six key recommendations that can help to solve the onboarding puzzle for all banks.

#### **1. Develop an onboarding process that meets customer expectations and eliminates all channel breaks within the onboarding experience:**



Banks will continue to acquire more and more customers via digital channels. Thus, it is crucial to design an account opening process that matches the customer expectation, who is nowadays used to onboard for other digital services and platforms like Spotify, Instagram, Amazon and others in a seamless way. What the before-mentioned services have in common is that they try to prevent any break in the channel during onboarding, but also within other customer journeys. Banks need to work on paperless onboarding processes as well as processes for which no physical signature is required. Every break in the channel will decrease customer conversion and satisfaction and likewise increase cost of the process.

#### **2. Make required onboarding information and prerequisites transparent and understandable for the customer:**



The potential customer needs to know upfront, right before the start of the onboarding process, what the bank expects from the prospect. Clear information and communication are key, so that the potential customer has all relevant details at hand and can run through the process in a smooth way. Thus, transparency is of highest importance and can be considered as a quick win to improve the onboarding experience and customer conversion.

#### **3. Guide the customer through the onboarding flow and empower customer support to help prospects during onboarding in a quick and high-quality manner:**



Another quick win for the banks is to improve the happy flow for prospects with guidance through the onboarding flow using, for example, progress bars, simple explanations and information boxes. The prospects should always know where they are currently positioned within the process and find information quickly, in case they do not understand why the bank is asking for certain information or why the bank requires the prospect to use a certain identification method. With regard to the unhappy flow, we found out that the employees were not able to answer rather simple questions in a high-quality manner [4]. A lack of knowledge and training



on customer support level is critical and needs to be solved by almost all banks that we have assessed.

#### 4. Make use of tools that ease the process of data entry and eliminate errors:



In order to limit drop-out rates during the process, banks should make use of more auto-filling and other tools to make data entry by the prospect as quick and easy as possible. Additionally, errors can be prevented by various in-process validation tools to increase conversion and also to reduce manual efforts by the bank, leading to cost reduction.

#### 5. Enable customers to instantly login and start using the payment account after successful onboarding:



Customers are used to instant onboarding experiences from other digital services. Thus also in banking, the customer should be able to select the login credentials (e.g. PIN or username & password) during onboarding and instantly use them to login and interact with the service.

However, some banks don't give the customer the option to select the login details themselves and most banks need a few hours to a couple of days to fulfil KYC / compliance and other relevant checks.

#### 6. Deliver a consistent look and feel throughout the whole onboarding experience:



A good UX is not only a matter of user interface design, but rather indicates a logical flow of the onboarding boarding process, relevant for the target customer. Simple, understandable and consistent look and feel needs to reflect the overall brand strategy and product/services offered.

1 Waiting time for the customer after the identification process until he/she gets a response form the bank with information about the status of his application.

2 Any switch of channel that interrupts the seamlessness of the onboarding process – i.e. a switch from digital to a non-digital channel (manual hard break) as well as a switch between digital channels (digital break) that can occur actively (where the prospect needs to get active to switch the channel) or passively (where the prospect is passive during the channel break).

3 To evaluate the unhappy flow of the onboarding process we included an investigation of the customer support service of all analysed banks in respect to its knowledge about the onboarding procedure.



### Authors

Joris Eckrich, Tian Genthner

[ORIGINAL BLOG](#)[BACK TO INDEX](#)[SUBSCRIBE FOR NEWSLETTER](#)





## ONBOARDING IN FINANCIAL SECTOR

# Open Banking and TPPs trigger banks to innovate their corporate onboarding processes

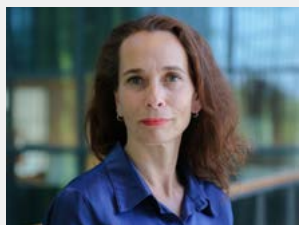
Josje Fiolet, Esther Groen on September 19<sup>th</sup> 2018



**Josje Fiolet**

Senior Manager and  
FIn Tech Lead

[GET IN TOUCH](#)



**Esther Groen**

Partner and  
Lead Banking

[GET IN TOUCH](#)

**PSD2 has been an important catalyst for banks to open up. While many banks in Europe are still focused on making the PSD2 deadline of September 2019, we see some leading banks move beyond compliance and shift towards Open API Banking. In this emerging Open Banking play, banks start to understand that enabling secure access to customer data is the new money, an outstanding customer experience is pivotal, and trust is the primary condition.**

The benefits of Open API Banking are multifold, however, they require collaboration with third parties to enrich the customer journey and introduce new financial services based on data. This forces banks to rethink their strategy for client products and services and manage the challenges that come with opening up. When collaborating with third parties, differences in for instance client segments and value propositions, compliance, quality of service and last but not least security protocols, will need to be tackled. Trust and confidence in the financial system can easily be damaged and breaking them can negatively influence the reputation of all parties involved.

With their economies of scale, banks can lay the foundation for an open trusted financial ecosystem in which they can safely collaborate with Third Party Providers (TPPs). To do so, a digital, secure and customer centric corporate onboarding process for TPPs is essential. It will enable banks to further commercialise their role of trusted advisor and create value in safeguarding their customers' identity and put them in control of sharing their data.

*Corporate onboarding essentially is about creating a customer identity for a new legal entity and charging it with all things required to deliver the requested product or service.*

**TPPs are a crucial success factor in creating customer value**

For corporate banks, the primary customer relationship is essential in maintaining a profitable and future proof business. Current corporate onboarding processes however are time-consuming, costly and deliver a poor customer experience. Already in 2014, Forrester research <sup>1</sup> demonstrated that the onboarding experience correlates with the profitability of practically all (98%) customer relationships. Deals are lost and business development rates are low. An outstanding onboarding experience will improve conversion rates, time to revenue and cross- and upsell, and, thus, contribute to customer value. With the financial industry opening up, onboarding becomes even more relevant as banks need to constantly prove their relevancy as other players will try to disintermediate existing client relationships.

PSD2 allows TPPs to access bank customers' payment accounts for Account Information Services (AIS) and Payment Initiation Services (PIS). Open Banking goes beyond PSD2 and allows

banks to create customer value by sharing customer (data) resources with TPPs in a secure way, through the use of open application programming interfaces (APIs). Consequently, banks need to onboard TPPs and, since they have all kinds of corporate identities (f.i. financial institutions, BigTech, FinTech, Retailer, SMEs), several corporate onboarding processes will apply.

For regulated PSD2 services, a standard procedure on how to onboard TPPs is prescribed in the Regulatory Technical Standards (RTS). However, for Open Banking no standards apply. The diversity of TPPs and functionality of APIs is unfamiliar territory for banks. As this impacts the risk profiles and the KYC obligations and attributes needed to charge the corporate TPP identity, banks tend to be hesitant and fall back on their existing processes.

However, instead of onboarding TPPs via the existing siloed, cumbersome, and costly processes, banks should seize this opportunity and design a modular, digital, and secure TPP onboarding process.

**How to best seize the opportunity and innovate corporate onboarding**

When innovating corporate onboarding, all types of TPPs and APIs offered should be considered. It is therefore important to start with 'the end in mind' and go for flexibility. Where current onboarding processes are often static, new processes should consist of generic building blocks that can be deployed depending on f.i. TPPs identity, services offered, type of APIs offered by TPP and the risks involved. This results in a flexible onboarding architecture as depicted below.

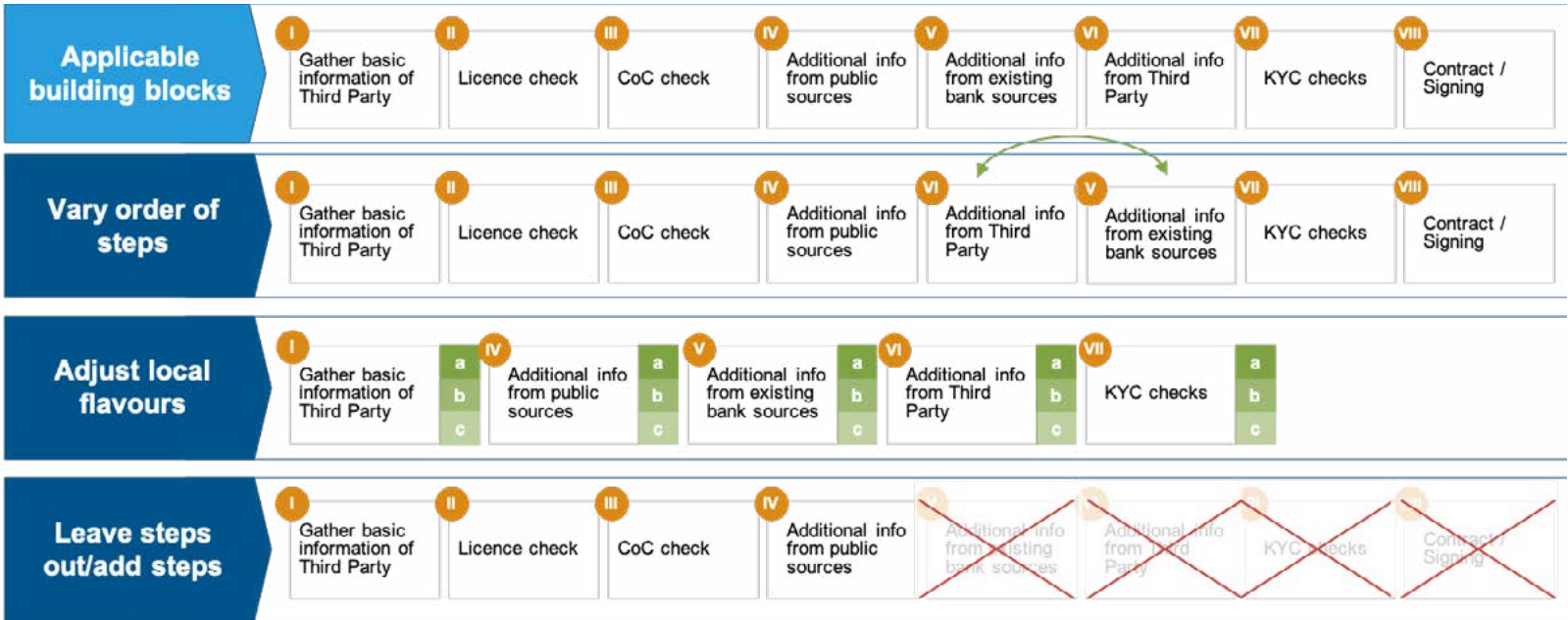


Figure 1: Architecture design onboarding in the PSD 2 and Open Banking landscape, INNOPAY 2018.



The onboarding process should aim for convenience and ease of use, while gathering all attributes required, minimising risks, and adherence to KYC obligations where needed. A flexible architecture therefore comprises of:

1. **Variation in the order of steps:** offer a relevant and tailored onboarding experience;
2. **Adjust to local flavours:** f.i. KYC requirements could be a quick check against sanction and PEP lists, but could also include full identification procedures;
3. **Leaving out steps:** when onboarding a TPP that offers APIs with limited risk exposure, f.i. finding the nearest ATM, there is no need for building blocks 4 –7. When a TPP offers PSD2 APIs only, you are only allowed to apply building block 1.

In short, with the PSD2 compliance agenda slowly dropping in priority, banks should start with designing and implementing a digital, secure and customer centric onboarding process for all TPP identities. An important step for banks to further leverage their role of trusted advisor, create value for their customers through API's and strongly position themselves into the Open Banking play.

1. Source: Client-Centric Onboarding, Hopes and Realities For Global Banks – Forrester (2014).



## Authors

Josje Fiolet, Esther Groen

[ORIGINAL BLOG](#)[BACK TO INDEX](#)[SUBSCRIBE FOR  
NEWSLETTER](#)

# Get in touch!

## The Netherlands

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

[SEND AN EMAIL](#)[VISIT OUR WEBSITE](#)[CONNECT ON  
LINKEDIN](#)[SUBSCRIBE FOR  
NEWSLETTER](#)

© 2019 INNOPAY. All rights reserved.

