FINOLOGEE

DIGITAL FINANCE

Tips & Tricks for PSD2

Get PSD2-ready with Finologee

Tips & Tricks
for PSD2

Get PSD2-ready with Finologee

Latest news and updates about PSD2

Table of Contents

Introduction

Why this guide?

This guide provides some key insights on PSD2 implementation by payment accounts-holding banks - from a practical perspective.

01

We'll address questions *such as*

How to manage a PSD2 implementation project

What are the regulatory deadlines that banks will have to meet in 2019

What the concept of a sandbox is about

When and how Finologee can help you

Over the past year, we have helped our clients preparing the final stage of becoming PSD2-compliant, relying on the platform we have built since mid-2017. In the pages ahead, you will find some of the essential take-aways and learnings acquired through this process as well as some advice we wanted to share with you. At the end of this guide, you'll be able to get an overview of our value proposition in the PSD2 context, i.e. how we can help you with our 'PSD2 for Banks' platform.

Finologee gets a double ‘PSF de Support» license

Luxembourg’s Minister of Finance grants Finologee a double ‘PSF de Support’ licence (Art 29-1 and 29-4) on January 25th, 2018. Finologee will be supervised by the Commission de Surveillance du Secteur Financier (CSSF).

Minister of Finance Pierre Gramegna with Finologee CEO Raoul Mulheims

LUXEMBOURG IN FINANCE AWARDS 2018

FINANCE STARTUP OF THE YEAR

Who is Finologee?

Finologee is a Luxembourg-based FinTech and RegTech specialist focusing on building digital ecosystems for the financial industry. Finologee is the latest venture from the entrepreneurs that developed Digicash, the Luxembourg’s retail banks’ mobile payment product and network. Finologee runs a trusted digital platform that simplifies connectivity between financial institutions and a variety of fintech solution providers, essentially enabling an “App” repository for its institutional clients. Institutions can more easily source and implement components that have been verified by Finologee such as ID document validation, video chat, electronic signatures, access to bank account (PSD2), various KYC and remediation tools and messaging features. Finologee develops a variety of its own apps and aggregates best-in-class FinTech products into its platform.

"In a nutshell, it is an off-the-shelf and fully compliant product enabling banks to meet PSD2 requirements in the quickest and most efficient possible way."

How can Finologee help you with PSD2?

Finologee's "PSD2 for Banks" application enables any financial institutions holding payment accounts that are accessible via online channels to meet PSD2 regulatory requirements quickly and easily.
Finologee's application provides for all the services needed, access and authentication management.

The product relies on Finologee's FinTech Acceleration Platform, providing a high-performance environment for API access management, an authentication stack (implementing various third-party solutions) and consent management, multiple standards implementation (STET, Berlin Group, UK Open Banking), exhaustive documentation to third parties and a developer/TPP sandbox.

Hosting and technical management is done on Clearstream's infrastructure, with a variety of service level choices and guarantees. A full integration with Finologee's FinTech Acceleration Platform also offers additional internal and external apps and the opportunity for banks to expose and monetise their own APIs via the platform's marketplace.

Are you in scope of PSD2?

2 questions you should ask as a bank

02

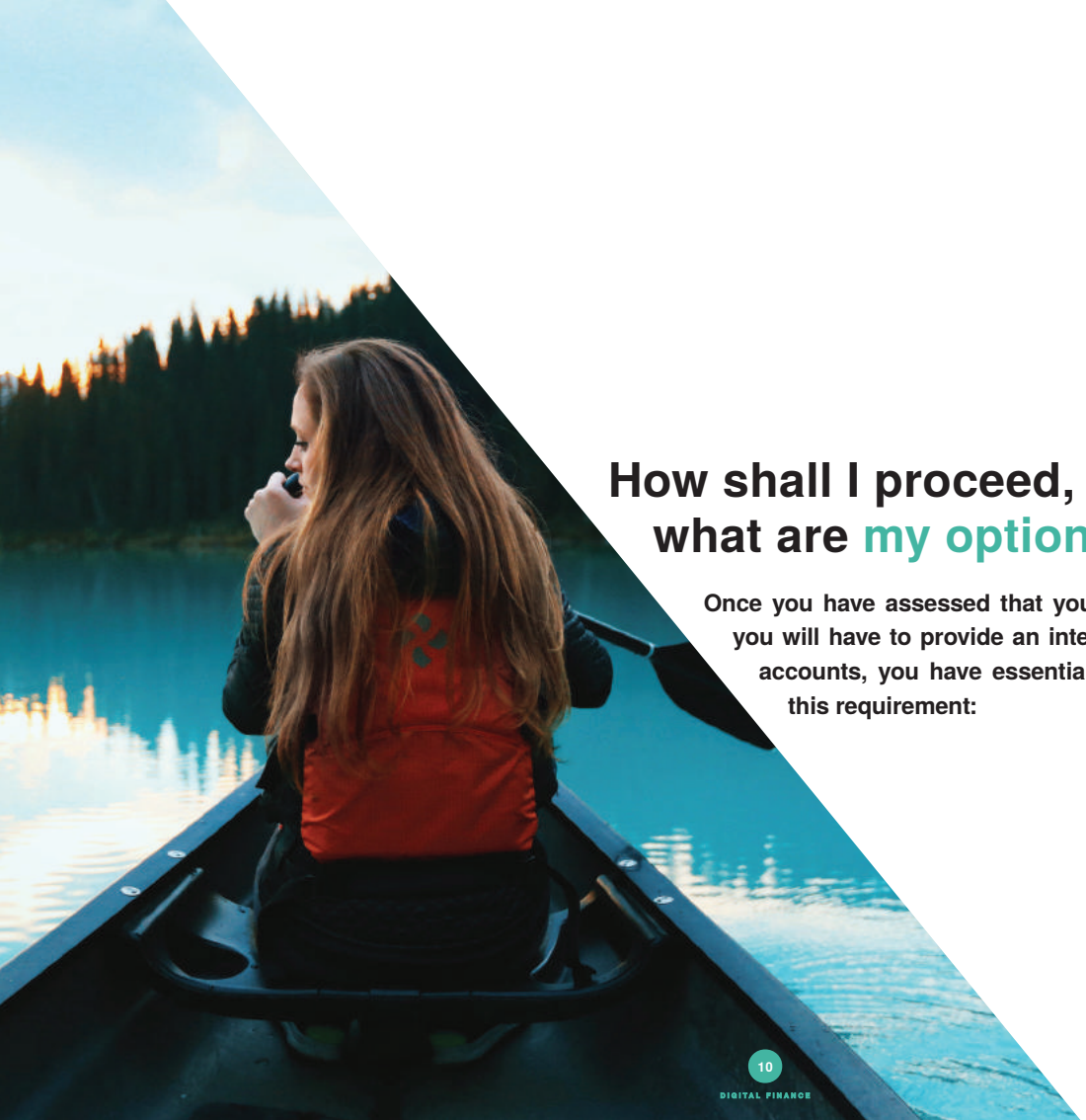
“Are my accounts *payment accounts*?”

If yes

“Are my payment accounts *accessible online*?”

Commission delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication:

(...) Recital (20): Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. (…)



How shall I proceed, what are my options?

Once you have assessed that you are in scope of PSD2 and that you will have to provide an interface to access your customers' accounts, you have essentially three options to comply with this requirement:

1

Develop your own PSD2 connectors and management environment

+ Full control
− High cost, expertise & maintenance requirements

2

Rely on a group or parent company solution

+ Potential cost optimisation
− Dependency & resources/priorities for implementation

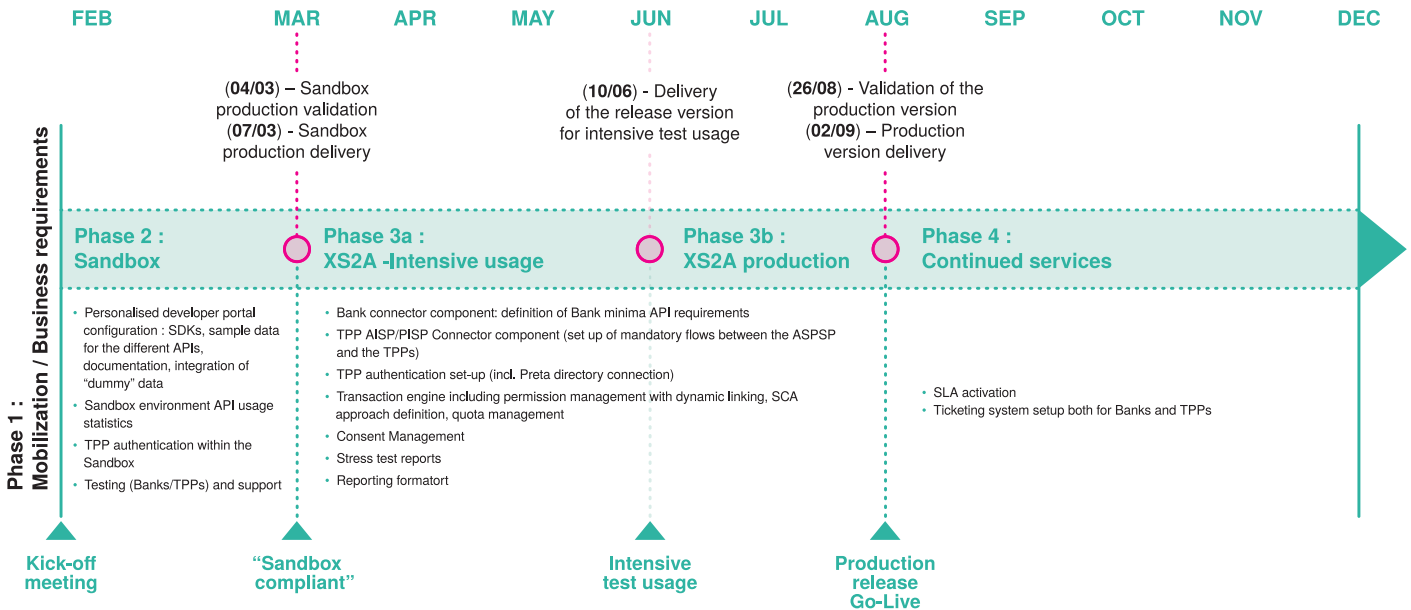
3

Use a shared PSD2 platform by an external provider

+ Lower cost, shared expertise, lower maintenance
− Less control, guarantees by external provider needed

What are the milestones of PSD2?

03


FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
(04/03) – Sandbox production validation
(07/03) - Sandbox production delivery
(10/06) - Delivery of the release version for intensive test usage
(26/08) - Validation of the production version
(02/09) – Production version delivery
Phase 1 : Mobilization / Business requirements
Phase 2 : Sandbox
Phase 3a : XS2A -Intensive usage
Phase 3b : XS2A production
Phase 4 : Continued services
• Personalised developer portal configuration : SDKs, sample data for the different APIs, documentation, integration of "dummy" data
• Sandbox environment API usage statistics
• TPP authentication within the Sandbox
• Testing (Banks/TPPs) and support
• Bank connector component: definition of Bank minima API requirements
• TPP AISP/PISP Connector component (set up of mandatory flows between the ASPSP and the TPPs)
• TPP authentication set-up (incl. Preta directory connection)
• Transaction engine including permission management with dynamic linking, SCA approach definition, quota management
• Consent Management
• Stress test reports
• Reporting formatort
• SLA activation
• Ticketing system setup both for Banks and TPPs
Kick-off meeting
"Sandbox compliant"
Intensive test usage
Production release Go-Live
Expected release date
Project milestones

Get PSD2-ready with Finologee

In this section, we will take you through a selection of articles written by our experts to address the main challenges PSD2 will bring for your business.

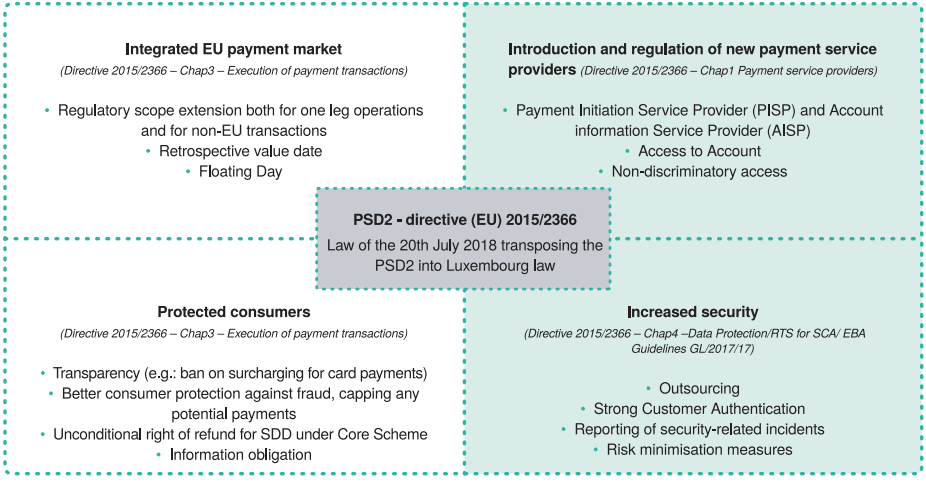
04

What are the PSD2 reporting requirements for banks?

October 19th, 2018

Did you know that the scope of the changes introduced by the **PSD2** actually **goes far beyond introducing APIs** and forcing banks to provide **access to their customers' accounts** to third party providers (TPPs)?

Indeed, much has been written about the introduction and regulation, enforced by PSD2, of new payment service providers. This paradigm shift has sometimes overshadowed other key principles introduced by the Second Directive on Payments such as, new rules around European payment market (one-leg operations, retrospective value date, floating day), protection for consumers (transparency, information obligation), and more specifically **reporting requirements**.



This is why banks (Account servicing payment providers - ASPSP) should carefully analyse their reporting obligations under PSD2 applicable since July 20th, 2018 (date of the transposition of the Directive into the Luxembourg Law) and anticipate their implementation.

Without being exhaustive, we have highlighted some important reporting aspects and tried to give some quick tips to help you getting ready:

Reporting under PSD2: three main challenges to handle

To prepare for the full implementation of the **Security measures for operational and security risks reporting** (RTS on SCA & EBA/GL/2017/17), ASPSPs should proactively define a risk management framework, including a security policy document. Besides, defining the required procedures and systems to identify, measure, monitor and manage the range of risks stemming from the payment-related activities of the PSP and to which the PSP is exposed to (including business continuity arrangements) is part of the process leading to an accurate security risk reporting framework and setup. Finally, ASPSPs should not forget to ensure the effectiveness of the security measures set out in the RTS guidelines when operational functions of payment services, including IT systems, are outsourced.

Major incident reporting (EBA/GL/2017/10) also has to be handled by ASPSPs under PSD2. In order to meet PSD2 requirements, ASPSP should proactively set up process to classify incident based on impact level criteria, define an incident notification process (including initial, intermediate and final report) and review internal operational and security policy.

"ASPSPs should not forget to ensure the effectiveness of the security measures set out in the RTS guidelines when operational functions of payment services, including IT systems, are outsourced."

Last but not least, **Fraud Reporting** (EBA/GL/2018/05) represents one major pillar of reporting requirements under PSD2. In that perspective Banks need to set up processes and tools that enable them to monitor unauthorised payment transactions, including as those processed as a result of the loss, theft or misappropriation of sensitive payment data or of a payment instrument, and report unauthorised payment transactions to the regulator (including statistical information per payment channel and authentication methods).

In the light of PSD2 requirements, and if not done yet, ASPSPs should ask the right questions: am I able to manage this internally, knowing that IT, risk management and compliance teams would have to work in close collaboration? Or do I prefer to rely on a consultancy firm aiding with change and reporting management?

How to implement Strong Customer Authentication?

November 5th, 2018

Strong Customer Authentication (SCA) - Transaction Factors

Something only user knows

Password, pin code...

Something only user possesses

Smartphone, token...

Something only user is

Finger print, face recognition...

One of the major implications of PSD2 is the focus on improving security in the payments space by emphasising Strong Customer Authentication (SCA). This article aims to provide some guidance to the Payment Service Providers (PSP) for an appropriate implementation of the European Banking Authority's (EBA) legal requirements concerning SCA. As a part of its "PSD2 for Banks" product, Finologee not only offers three solutions for SCA, but also a SMS OTP based solution - which has recently been validated as a valid authentication factor by the EBA.

Taking into consideration the rapidly rising number of online operations (mainly related to access to payment accounts for online and electronic transactions), the second Payment Services Directive (PSD2) has reinforced the rules related to Payment Security. In this context, all Payment Service Providers and in particular banks or account servicing payment service providers (ASPSP) are required to implement **Strong Customer Authentication (SCA)** that include elements that **dynamically link the transaction to a specific amount and a particular payee**. In addition, as described in our previous article "PSD2 reporting requirements for banks", banks must also provide fraud and security-related incident reports to the regulators.

What is Strong Customer Authentication and dynamic linking?

To be compliant with the SCA definition under PSD2, the authentication method available for the Payment Service User (PSU) must integrate, at least, the use of two (two-factor authentication) of the following **three elements**:

1. **Knowledge:** a component which is only known by the PSU, such as password, PIN code or response to a security question;
2. **Possession:** a device that only the PSU owns, such as a hardware token or a mobile phone;
3. **Inherence:** something which is unique and linked to the PSU, such as finger print or facial recognition.

Strong Customer Authentication (SCA) Transaction Factors

Furthermore, the concept of "dynamic linking" has been introduced to guarantee the integrity of transaction validation. This concept imposes that the payer must be made aware of the amount of the payment and of the payee during the authentication process. This is necessary to avoid any "man-in-the-middle attack" which could modify the details of the transaction.

Payment Service Providers can obtain further details on SCA and dynamic linking by consulting the chapter 2 of the final version of Regulatory Technical Standards (RTS) on strong customer authentication (SCA) and secure open standards of communication (CSC). Additionally, the EBA has made public a Q&A tool on PSD2 and more explicitly on the SCA subject.

What is Finologee's approach towards SCA and dynamic linking?

Finologee has built a **state-of-the-art transactional and authentication/authorisation platform** that handles interactions between banks and their counterparts in strict application of the revised payment service directive (PSD2) and its Regulatory Technical Standards (RTS) on strong customer authentication (SCA) and secure open standards of communication (CSC) published in the Official Journal of the European Union, guaranteeing their partner banks full regulatory compliance in this new state of play.

As part of its **"PSD2 for Banks"** product, Finologee offers a ready-to-use platform for API access management of AISPs and PISPs, with an authentication and authorization stack. This module can support redirect SCA Approach using OAuth2/OIDC, Decoupled SCA Approach, Embedded SCA Approach without SCA method, Embedded SCA Approach with only one SCA method available, Embedded SCA Approach with selection of a SCA method.

In view of this, Finologee can:

- **Implement LuxTrust**: mainly for local Luxembourg players. If the bank is using LuxTrust as an authentication method, no additional integration needs to be done. Finologee can connect directly to Orely and supports all authentication methods provided by LuxTrust.
- **Connect to various third-party SCA protocols** based on standards such as OAuth2, OpenID Connect, SAML2 or any proprietary protocol such as Vasco or RSA APIs.

mpulse
mobile payment & messaging

In addition, thanks to **Mpulse** - Finologee's sister company, operating Luxembourg's central SMS payments and routing gateway since 2006 - Finologee can provide banks with **a SMS OTP solution** which is considered as an authentication factor by the EBA. Indeed, the EBA has recently clarified that "For a device to be considered possession, there needs to be a reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device". In this context, a one-time password sent via SMS would constitute a **possession element** and should therefore comply with the requirements.

In parallel, the RTS lists a **series of exemptions** for which the bank might decide not to apply strong customer authentication. These exemptions include payments for small amounts, parking or transport fares, payments to trusted beneficiaries or to a different account of the same user. Within Finologee's PSD2 solution, rules on when exactly exemptions to SCA should be applied can be defined and **customised on a per-bank basis**.

Finally, to become PSD2 compliant, some banks have decided to completely change their customer authentication method. But before choosing such a drastic approach, a in-depth **analysis of the SCA tool** could be first performed to avoid any additional or unnecessary costs. Banks must also be aware of complementary and/or alternative solutions which could enrich their current SCA solution in order to fully fulfil RTS requirements.

What is the PSD2 Sandbox environment?

November 30th, 2018

Even though the technical access to account obligations introduced by the PSD2 Directive will become effective only as of September 2019, **banks must meet some "pre-go-live" requirements by 14th March 2019**. By this date, **banks need to make sure that the technical specifications of the interfaces shared with or made available to third party providers (TPPs) are documented**. In essence, **banks must provide a** so-called **'sandbox'**, i.e. a testing environment, **to TPPs so they can carry out tests of the software and applications** they develop for their customers and end-users.

But what exactly is expected from banks?

How can Finologee's solution help to reduce efforts on the banks' side?

What needs to be made available for TPPs in the next 3 months?

This first deadline (14th March 2019) can be seen as a first attempt of friendly cohabitation between two strangers, banks and TPPs. They do not know each other quite yet, but they have to get acquainted to jointly fulfil the payment services users' needs. Basically, banks (ASPSPs) have to make sure that the technical specifications of any of the interfaces are documented, i.e. by specifying a set of routines, protocols, and tools needed by payment initiation service providers (PISP), account information service providers (AISP) and payment service providers issuing card-based payment instruments to allow their software and applications to interact with the systems of the ASPSP.

- Banks must make the documentation available - at no charge - to all Third-Party Providers (PISPs, PISPs issuing card-based payment instruments and AISPs) that have applied with competent authorities for the relevant authorisation or licence. They also have to publish a summary of the documentation on their websites.
- A testing environment, with support services, for connection and functional testing will have to be deployed to enable authorised payment initiation service providers to test their software and applications used for providing payment services to users. However, no sensitive information from banks should be shared through the testing facility.

How can Finologee help Banks to be ready for the 14th of March?

As a part of its "PSD2 for Banks" product, Finologee includes a developer portal providing consolidated developer resources with a **single point of contact for all documentation**, **how-tos**, **tutorials**, **examples**, **code samples**, **and SDKs**. Finologee's sandbox is the place where the TPP can sign up and manage its subscription, define the APIs and versions that he wants to use, and it provides access to premium APIs, billing and invoicing overview of API usage. It is an **easy entry point for accessing APIs** of all banks connected. The sandbox is exposed through the developer portal and lets the TPP test its application before going into production. The sandbox environment contains sample data for the different APIs that cover most real-life scenarios that the TPP may encounter in a production environment.

Effectively, **only very few efforts are required on the bank's side** at this stage. Only the definition of sample data to be used in the sandbox will be needed from the bank. Finologee's approach is aligned with the two phases required by the PSD2 and related regulation. Indeed, Finologee intends to release a sandbox environment where no technical resources, efforts or interconnection works are required on the banks' side.

By using Finologee's solution banks can thus benefit from a **3-month buffer** and then focus their efforts on the deployment of access-to-account connectivity and environments that will have to be **ready by September 2019**.

How to deploy your PSD2 project?

December 12th, 2018

Choosing a suitable strategy and deciding on a provider to work with is one thing for banks that need to address the PSD2 topic. Implementing the chosen approach is another one. Based on our experience with payment infrastructure projects (Digicash), the joint planning efforts with our clients that are currently being carried out and the feedback they gave us, there are some **key takeaways that may help to operate a smooth project management process while making sure the compulsory PSD2 deadlines are met**.

Given the services we provide and the typical setup we observe in these contexts, we will focus on the scenario of a joint implementation by a bank using a hosted PSD2 platform such as Finologee's "PSD2 for Banks" product. Nevertheless, most of the topics and issues listed hereafter also apply to PSD2 implementations handled by banks with their own teams or to custom on premise deployments by IT suppliers.

1 Put the right stakeholders around the table

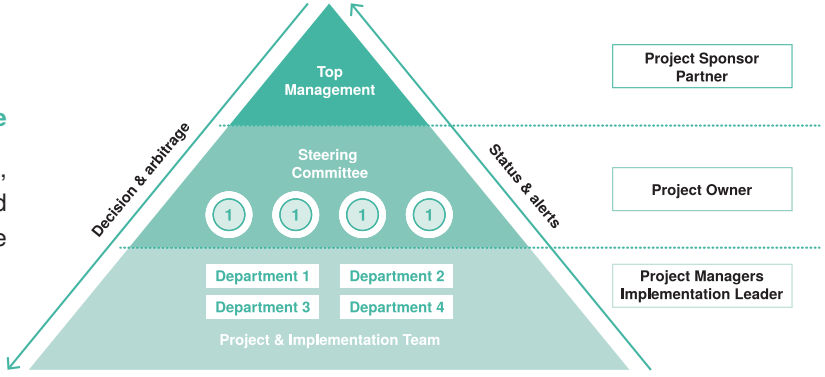
Irrespective of the fundamental strategy chosen, i.e. either developing an in-house solution or opt for a third-party product, implementing a PSD2 framework requires mobilising various departments within the bank, because of the directive's substantial impact on the payment infrastructure and the scope of requirements and related features (as an example, see our recent article "Banks: have you accurately anticipated PSD2 reporting requirements?").

Because of this wide array of topics and challenges to address it is **key to have (all) the right people on board from the start**. IT teams are of course at the core of each PSD2 project and IT managers, architects and security experts will do the heavy lifting, but the involvement of compliance and business teams - as well as of the payment specialists of course - from the beginning is essential to maximise the efficiency of any PSD2 compliance project.

From our experience, it often also makes sense to appoint an external advisor to help both with the gap analysis and/or the project management on the bank's side. This can help to minimise risks and increase efficiency.

2 Define a strong & suitable project governance

Because of the diversity of stakeholders involved, we highly recommend setting up an efficient and transparent **project governance** with well-defined role assignments:



+ Ideally, there should be a **project owner**, holding the keys to the bank's departments, with direct access to management and all relevant stakeholders. This main contact person should have the required knowledge and be empowered by the bank's management.

+ A project sponsor at the bank's **top management** level will most certainly be helpful over the course of the project: PSD2 has an impact on strategy, there are going to be moments in time when strategic input will be required and choices will have to be made, also given the spill-over potential of PSD2 on CRM, customer retention/volatility and other topics. The project sponsor's role will also be important if frictions between departments or stakeholders occur to avoid inefficiencies or lack of decision-making ability, especially given the limited timeframe for PSD2 implementation.

+ **All relevant departments** should assign a main point of contact the project manager should refer to. This person should of course also assist to steering committees if their presence is required.

+ The **technology partner should make sure to shadow the different roles**: a competent project manager knowing their way around PSD2, a strong technical lead empowered to make decisions and having a substantial experience in this kind of projects, and of course a project sponsor at the supplier's management, if not a partner in the company.

It seems rather obvious that project managers on both sides should lead and coordinate the project over time. One important lesson we also learned over the last few years is that interacting directly with departments and stakeholders inside the bank as an external supplier certainly has its benefits. But the project management role should always be in control and refrain from "leaving it (only) to the specialists" to handle specific tasks or address challenges. Too often this leads to inefficiencies and questionings about roles and responsibilities, as the specialists do not always consider the big picture and have different priorities.

Finally, **for complex project setups involving several entities** in different jurisdictions, it becomes even more important to designate **primary contact persons**, clearly outline roles and responsibilities, goals and expectations, and of course make sure to agree on the overall timeline and dependencies.

3 Beware of the pitfalls and tricky issues

First, there are quite a few PSD2 requirements one should not underestimate, because of their complexity and/or because of the workload entailed. While a third-party PSD2 Platform will handle the main part of the regulatory requirements out of the box, some **substantial efforts are still required on the banks' side** to enable, given the nature of the features to be implemented:

+ A connection to the bank's backend/payment systems is required, to initiate and validate payments and retrieve account information to be provided to the TPP,

+ The bank's authentication mechanism must be linked to the provider's authorisation platform to provide SCA functionality,

+ Finally, the security aspects will also require some efforts on the bank side. Indeed, a secure and trusted connection should be used (such as TLS mutual authentication, IPSec VPN, OpenID Connect)

Secondly, **some PSD2-related issues are not fully 'stable' yet**, in terms of definitions, analysis or because of the lack of position statements by relevant authorities such as the EBA or the regulators. Here are a few examples:

+ Conditions for a fall-back mechanism under PSD2 and conditions to benefit from an exemption from the contingency mechanism (a last opinion has been published by the EBA on December 4, 2018)

+ PSD2 technical specifications (such Berlin Group or STET) keep evolving – stabilized version would probably be expected only for the second quarter of 2019

In addition to this, because of the existence of certain grey areas in the PSD2 sphere that have not been fully addressed by

the EBA, the ECB or national regulators quite yet, an essential recommendation for project managers and solution architects in charge of PSD2 implementations is to place the RTS and their updates on the top of their reading lists for the coming months, and to keep an eye on any relevant EBA papers and PSD2 position statements from regulators.

4 Keep the PSD2 deadlines in mind

In order to accurately anticipate **the three main PSD2 milestones set out for 2019**, we strongly advise to define a suitable roadmap, starting from the known deadlines and working your way back to the present time. Again, this might sound quite trivial, but this allows you to gather the required elements, approvals and input proactively, as well as to be prepared for the next step. For example, as of today, business requirements definitions and sandbox implementation should already have been kicked off, including SDKs, sample data for the different APIs, documentation and integration of this sample data. As a next step, the most intensive phase of the project will be held between March and June 2019.

To know more about the milestones of PSD2 please refer to section 3 of this guide.

5 Do not underestimate the project workload

As stated above, PSD2 deployment within a Bank requires the involvement of various functions: project, IT, compliance and business. Given the fact that there are absolute deadlines to be met - if you do not want to be subject to penalties - coordination, anticipation and a thorough project and priorities management are highly recommended.

PSD2 Compliance is about opening up your payments infrastructure to third parties. This comes with multiple layers of complexity and a variety of challenges. Even when choosing and external platform solution, the overall workload should not be underestimated, especially given the fact that some tasks can only be carried out sequentially and require some strategic decisions.

One more for the road, at a more strategic level: start your thinking process early enough to specify what your position in the market and **your strategy in a post-PSD2** world will be.

+ Do you want to play offense, or is it more a defense game you want to go for?
+ Do you want to empower your clients to actively use PSD2-based features with TPPs?
+ Do you envision to expose additional data sets, features or products via API, beyond PSD2?
+ What will be your strategy partnering or competing with your peer banks, how much do you want to – and how much can you afford to – rely on them or depend on their strategic choices?

Outline of Finologee's value proposition

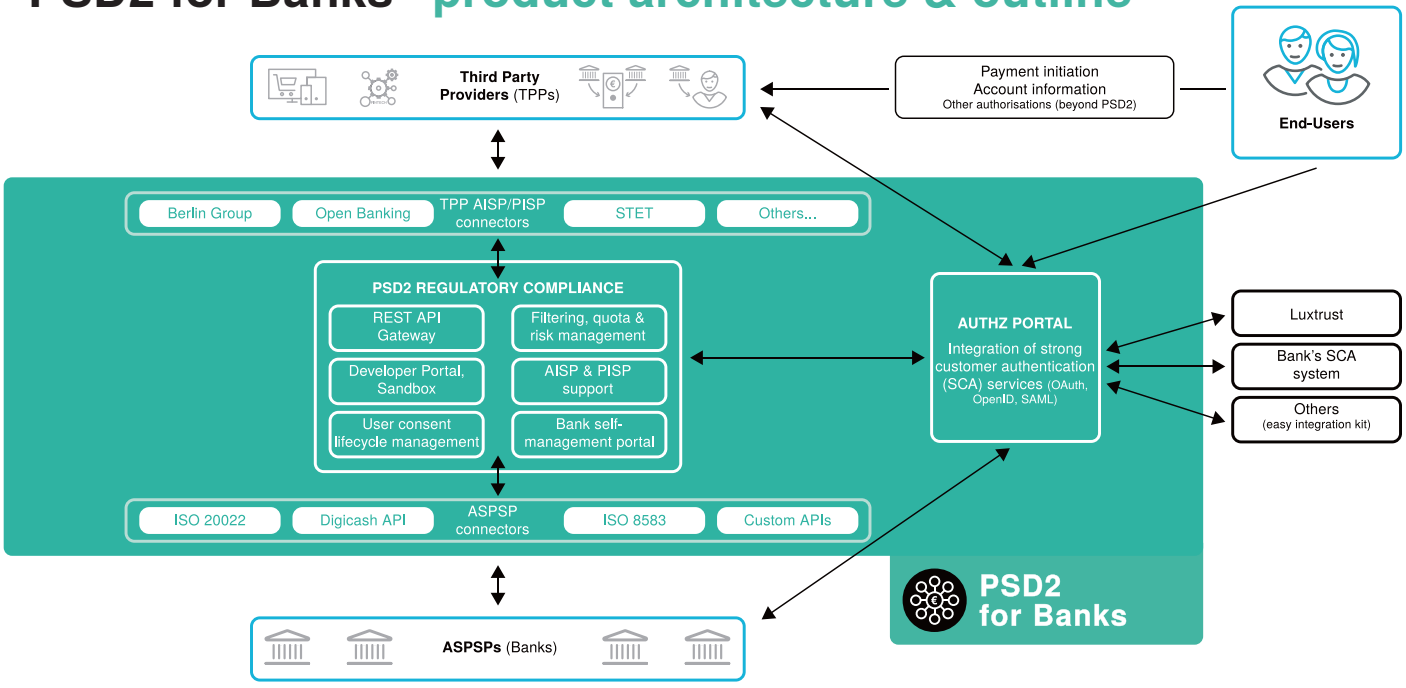
05

"PSD2 for Banks" what is it?

It is a state-of-the-art transactional and authentication/authorisation platform that handles interactions between banks and their counterparts in a PSD2 context for full regulatory compliance.

- Fully hosted product (Clearstream)
- Full range of compliance services
- Flexible SCA integration (including Luxtrust)
- Easy service/API enrichment
- Multiple standards (STET, Berlin Group…)
- International connectivity and compatibility

"PSD2 for Banks" product architecture & outline



Main features – components

1 REST API Gateway

- Exposure of standard APIs following the technical specifications of the Berlin Group and optional exposure to the technical specifications of the UK Open Banking initiative and of the STET group
- API Lifecycle management (efficient management of multiple versions)

2 AISP/PISP Authentication

- Validating the identity of the connecting AISP/PISP
- Various authentication & validation mechanisms (TLS, eIDAS, connection to Preta directory services)

3 Strong Customer Authentication

- RTS-compliant SCA OAuth2, OpenID, SAML, Luxtrust, others
- Token generation and validation
- Custom SCA-compliant modules for web/mobile banking

4 Consent Lifecycle Management

- Manage access tokens lifecycle
- Fine-grained permission management with dynamic transaction linking

5 Filtering & Quota Management

- Validating business rules laid out in the RTS: SCA requirements and exceptions, access rules and restrictions
- Quota management : enforcing RTS call quotas & response caching

6 Developer Portal:

- Single point of contact for all documentation, how-tos, tutorials, examples, SDKs, access to premium APIs & single interface for all banks
- Sandbox: isolated & feature-complete test environment for TPPs

7 Bank connectors

- Can use proprietary bank connectors
- Support for Swift, ISO 20022, REST, SOAP, or socket-based protocols & use existing authentication protocols
- Match bank's connectivity requirements (fixed IP, VPN...)

8 Bank Back – Office Portal

- Web-based portal allowing access to API publisher view and to analytics and statistics: detailed information on API usage with call count, number customers impacted, Tx volume, TPP distribution and profiles etc.
- Monitoring and SLA management

9 Support & service Level Agreement

- Support for AISP/PISP: provide email support
- Support for banks: email/phone support
- SLA defines response times, platform uptime, alerting, incident response

USP – What you'll get with us

1 One-stop-shop for best-in-class Fintech

- Transparent selection, due diligence and aggregation of best-in-class FinTech suppliers & sub-contractors: making them compliant with LUX regulation
- Continuous Research and Development

2 Flexibility & Performance

- Designed, built, maintained by the leading FinTech team in Luxembourg (the team behind the Digicash mobile payments product & infrastructure for retail banks)
- Continuous improvements & implementations, built on top of a high-performance FinTech Acceleration Platform

3 Total Neutrality

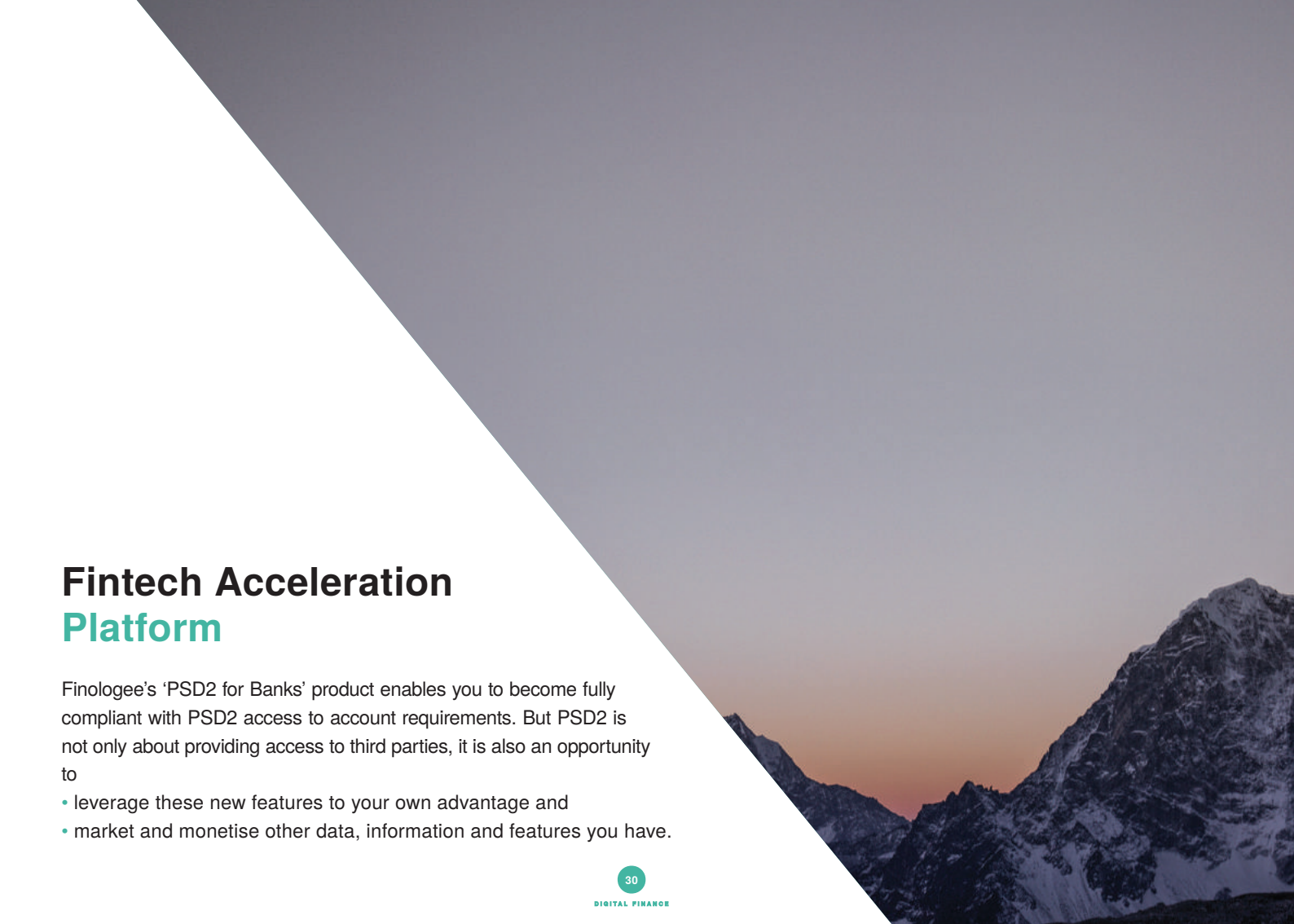
- No banking software/vendor/supplier dependency
- Fully neutral & independent shareholder structure, operations & development teams, no strategic conflicts of interest

4 Full regulation compliance

- Aligned with CSSF regulation, MLD4, PSD2, eIDAS, GDPR & others
- 'Support PSF' license (2 audit levels, right to audit, professional secrecy …)

5 High-end & compliant hosting and operations

- Hosting & infrastructure operations by Clearstream, a company managing some of the most critical infrastructures in the world (T2Securities & several stock exchanges)
- Complete outsourcing – full SLA coverage
- Operated under Luxembourg PSF licence (both Finologee & Clearstream)

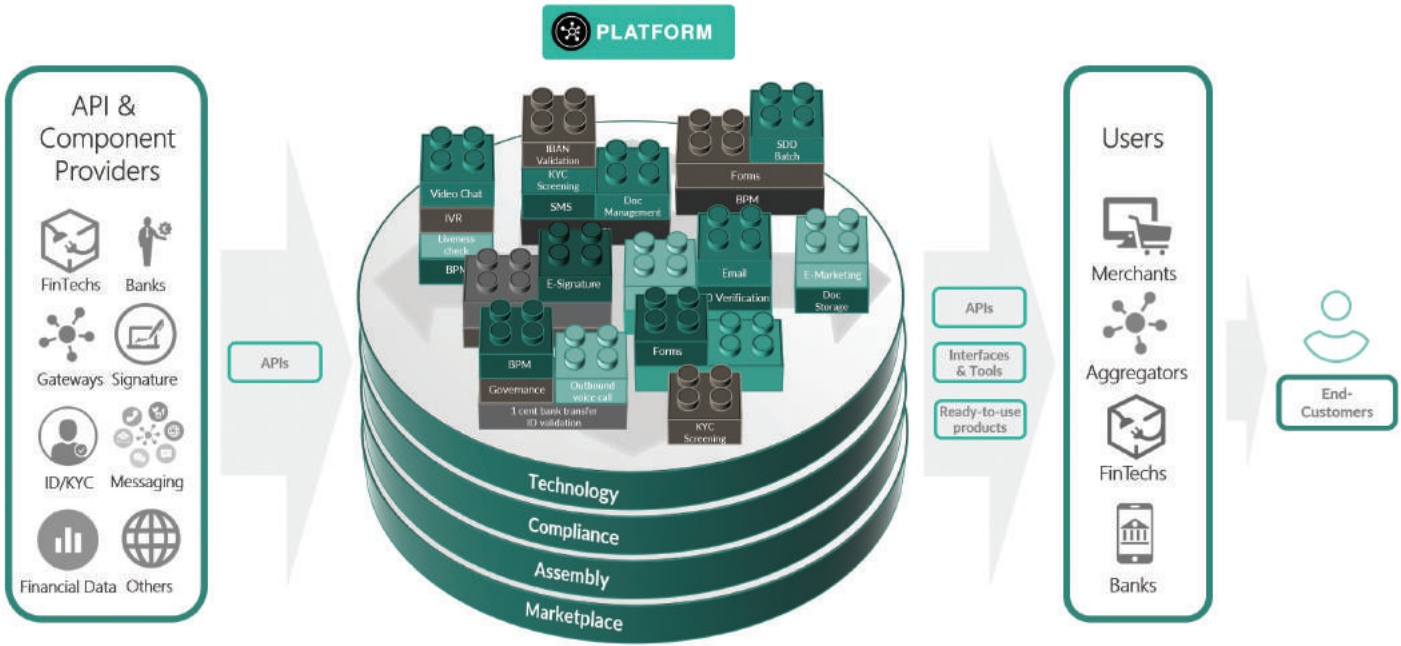


Fintech Acceleration Platform

Finologee's 'PSD2 for Banks' product enables you to become fully compliant with PSD2 access to account requirements. But PSD2 is not only about providing access to third parties, it is also an opportunity to

- leverage these new features to your own advantage and
- market and monetise other data, information and features you have.

The 'PSD2 for Banks' product is built on top of Finologee's FinTech Acceleration Platform. The goal of this platform is to create a **digital marketplace** and a leading-edge technical environment where FinTech companies and traditional financial services players give access to their services and expose their APIs for other users to build and enhance their own products. It is a high-performance infrastructure to host, aggregate, market, operate and expose own and partners' FinTech products and components, with a high-performance API gateway, an adequate billing and revenue share management system, all based on a hybrid cloud infrastructure, under a full 'PSF de Support' licence.



One-stop shop proposition

06

FINOLOGEE
DIGITAL FINANCE

Finologee is offering a PSD2 Compliance Product for banks using a single connection to bank systems. Indeed, Finologee is proposing a ready-to-use environment for API access management of AISPs and PISPs, with an authentication stack (implementing various third-party solutions incl. Luxtrust) for SCA and consent lifecycle management. Finologee is also handling multiple standards (STET, Group, UK Open Banking), the developer/TPP sandbox, as well as the filtering/quota management for Banks.

clearstream | DEUTSCHE BÖRSE GROUP

The infrastructure that hosts Finologee's software is run by Clearstream Services in Luxembourg. It is based on a state-of the-art fully redundant virtualisation environment. Clearstream is the operator of some of the world's most critical financial infrastructures (T2S network), and a renowned provider of application hosting for the financial industry. Finologee and Clearstream have joined forces to provide a high availability infrastructure for the hosting of FinTech/RegTech platforms, products and applications.

KPMG

Since the PSD2 topic came on bank's agenda, Finologee and KPMG are working in close collaboration to address the market needs: while Finologee brings its software solution, KPMG proposes to pilot implementation projects (PMO). On top of this optional project management and coordination activities, KPMG's role can be extended to software and solution architecture, testing, infrastructure implementation and managed services. KPMG is also able to produce and distribute reporting files and data required by PSD2 via its regulated PSF entity.

Reporting exemption request

07

Fallback exemption file assistance

As a bank that is in scope of PSD2 access to account obligations and provides a dedicated interface (API) to third party AISPs and PISPs, you have a direct interest in applying for the fallback exemption to avoid having to allow these third-party providers to use your standard web banking should your API be unavailable. We can help you with this file and the process, as part of the service offering tied to our 'PSD2 for Banks' product, in collaboration with KPMG regulatory and compliance services.

What is it?

An application file to be submitted to the regulator that contains details on:

- the assessment that the dedicated platform meets the RTS obligations (Article 32)
- availability and performance measuring of the dedicated interface
- how the 'widely used' condition by third-party providers is met

Why do I need it?

Most banks prefer to avoid that third- party providers rely on their regular web banking if their PSD2 API is unavailable because they do not want to expose their own interface and all the related data. Submitting a fallback exemption application file allows a bank not to have to expose its web banking interface as the backup solution to the main PSD2 API.

When do I need it?

Ideally, the first draft of the application file has to be sent to the competent authority before March 14th, 2019 in order to be ready with the PSD2 production platform by June 14th, 2019 and to be able to perform the 3-month period of intensive tests with the third-party providers. However, the file won't be fully closed until September 14th 2019.

How can you help me?

Finologee can provide you with all the information that is needed to demonstrate that the Platform accurately answers to the key performance indicators and service level targets. On top of this, KPMG can assist you with data consolidation, production of statistics, reporting about stress testing performed with third-party providers.

Get in touch with us

As a FinTech/RegTech player, Finologee is providing a “PSD2 for Banks” product and platform enabling any financial institution holding payment accounts to meet PSD2 technical requirements quickly and easily. “PSD2 for Banks”, its processes and flows have been designed and developed accordingly to match the PSD2, RTS and related provisions and obligations.

Finologee can help your bank comply with PSD2, as we do with dozens of other financial institutions.

For more information, please contact us by email at info@finologee.com or by phone at (+352) 27 75 08 1.

Georges BERSCHEID
Co-Founder – CTO

T (+352) 27 75 08-1
E georges.berscheid@finologee.com

Jonathan PRINCE
Co-Founder – Sales & Partnerships

T (+352) 27 75 08-1
E jonathan.prince@finologee.com

Mallorie RIBET
Product Manager

T (+352) 27 75 08-42
E mallorie.ribet@finologee.com

The content of this brochure is provided for information purposes only and is intended to serve as a general overview regarding the products and services of Finologee S.A.

Finologee is authorised under Luxembourg Law of 5 April 1993 on the financial sector and holds a 'PSF de Support' license (License number 06/19). Finologee is supervised by the Commission de Surveillance du Secteur Financier (CSSF).

DIGITAL FINANCE

FINOLOGEE S.A.
7, rue Jean Fischbach
L-3372 Leudelange
Luxembourg

T (+352) 27 75 08 1
E info@finologee.com
W www.finologee.com

RCSL B217.853
EU-VAT LU 2966 0355
PSF de Support 06/19