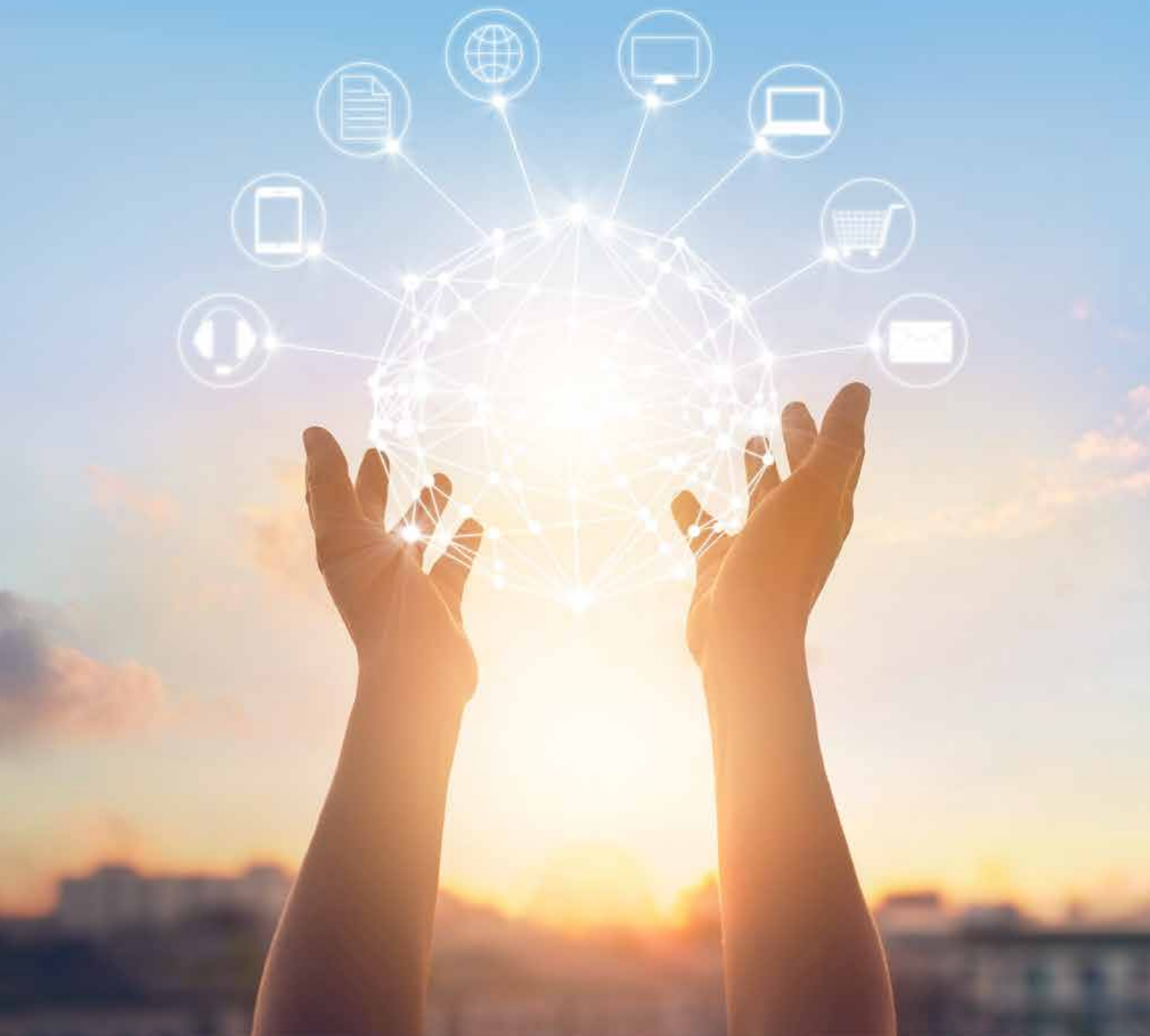
TEMENOS

THE BANKING SOFTWARE COMPANY

Payment Services Directive 2 (PSD2)



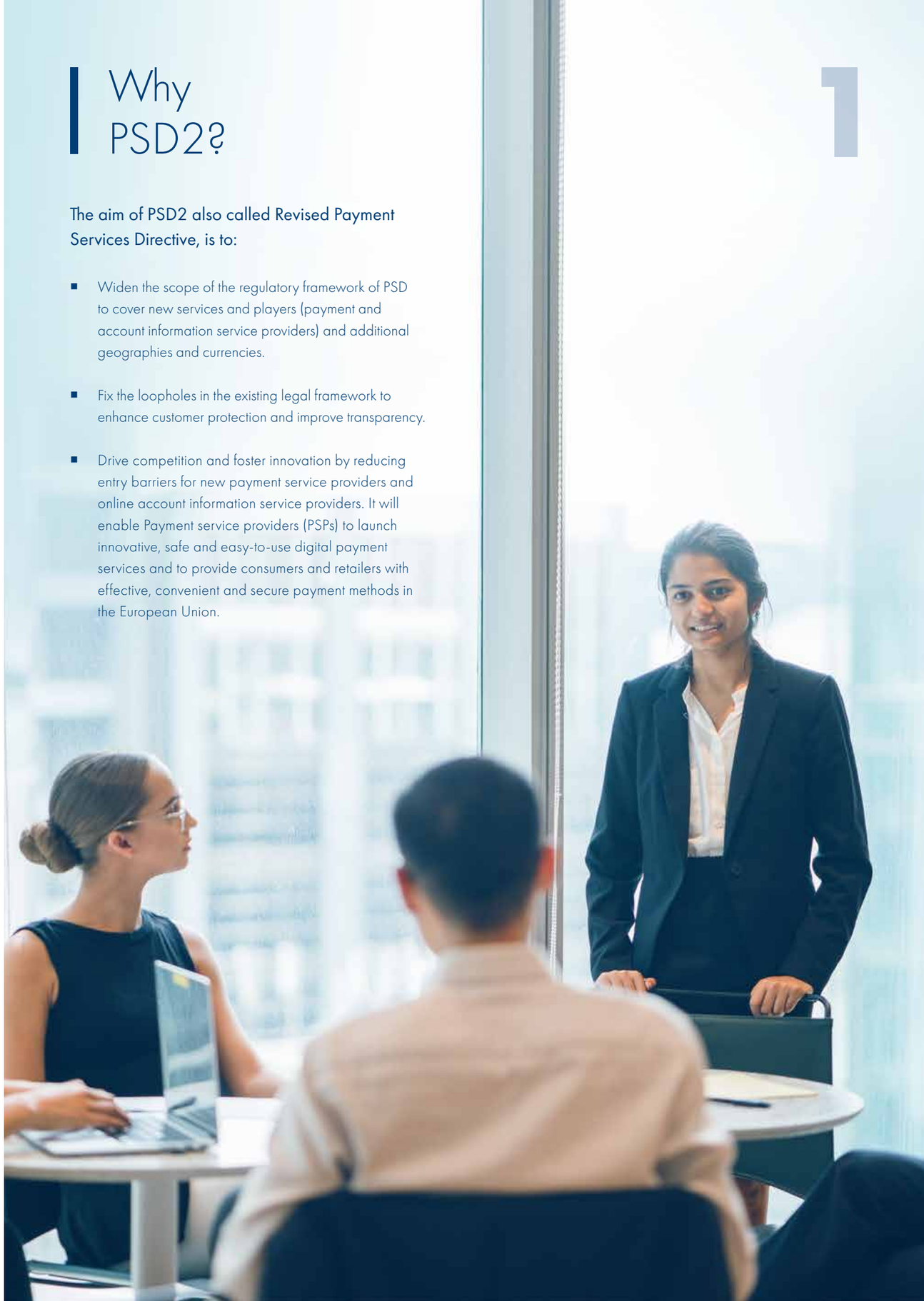
Contents

Why PSD2?

1

The aim of PSD2 also called Revised Payment Services Directive, is to:

- Widen the scope of the regulatory framework of PSD to cover new services and players (payment and account information service providers) and additional geographies and currencies.
- Fix the loopholes in the existing legal framework to enhance customer protection and improve transparency.
- Drive competition and foster innovation by reducing entry barriers for new payment service providers and online account information service providers. It will enable Payment service providers (PSPs) to launch innovative, safe and easy-to-use digital payment services and to provide consumers and retailers with effective, convenient and secure payment methods in the European Union.



Key Provisions of PSD2

2

PSD2 contains 117 Articles and covers a number of payment services. These services include:

- Enabling cash deposits and withdrawals
- Execution of credit transfers, standing orders, direct debits
- Payments through cards or similar devices
- Issuing of payment instruments (examples cards, wallets) and/or acquiring payment transactions
- Money remittances
- Payment initiation services
- Account information services

The list below is a selective set of provisions of PSD2, which impact payment service providers. There are several other provisions relating to card payments, thresholds for small payment institutions, registration and licensing, safeguarding requirements for funds handled, complaint and redressal procedures, etc. which should be analysed in detail for their impact by Banks.

PSD2

- Extends the application of PSD rules to "one leg out transactions" (where one of the Payment service providers (PSPs) is located outside European Economic Area (EEA)) to all transactions that start or finish in the EEA and, in any currency.
- Makes it mandatory for payment service providers to provide information on the terms and conditions for the service (execution time, actual or reference exchange rate and all charges payable with breakdown) to the payer, before execution and after execution of the payment, provide the actual exchange rate and charges (with breakdown) applied. ATM operators performing currency conversion should provide information to the payer of the charges and exchange rate applicable for such conversion before executing the transaction. These enhanced transparency measures seek to harmonise the information provided to users to enable them to make informed choices on the service provider.
- Widens the scope of PSD to include all types of payment acquirers (e-commerce, m-commerce platforms, large networks with payment volumes over 1 million euro per month) and all types of payment instruments, excepting those with limited network exemption (Examples - store credit cards, fuel cards, membership cards, meal vouchers, etc.).
- Seeks to provide customers a choice of service providers by mandating access to account information to Third Party Providers (TPPs) offering "Payment Initiation Services" (PIS) and "Account Information Services" (AIS). These new players by gaining access to customer accounts can offer services in competition to the existing banks with reduced costs.
- Introduces strong security measures compatible with the level of risk involved, including 2 factor authentication on all channels. Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) can rely on the authentication procedures of Account Servicing Payment Service Providers (AS PSPs) for seeking account information and initiating payment transactions. Banks will be required to provide access to information to third parties via APIs and strong (two factor) customer authentication. Any loss to intermediaries due to fraudulent transactions arising due to lack of strong authentication should be compensated by AS PSPs.
- Limits the liability of the payer to the maximum amount of 50 EUR, for any unauthorized payments due to lost or stolen payment devices. In case of unauthorized transactions, the AS PSP is responsible for compensating the payer, irrespective of whether the AS PSP or the intermediary was responsible for the unauthorized transaction.

European Council (EC) has mandated the implementation of PSD2 effective 13th January 2018.

What Impact Does PSD2 Have on Banks?

3

PSD2 presents a number of opportunities and challenges to banks.

For banks acting as payment processors, PSD2 mandates enhanced transparency and information requirements; charges are shared for transactions within the EU/EEA for payments in any currency and faster execution time for transactions in any currency. They will also face competition from new Payment Initiation Service Providers, who will offer services at reduced costs.

Banks should allow access to third parties, via an interface (API), to initiate payments from bank accounts. That access must be given on the same basis as if to account owner, i.e., if the owner can initiate a payment at zero cost, then so must a third party, with appropriate consents.

Banks have to ensure that they have the right infrastructure to support the Regulatory Technical Standards (RTS) on authentication and communication to be published by European Banking Authority (EBA) in summer 2016.

Allowing access to third parties potentially has profound consequences to banks, as it may reduce their ability to use current account relationships as gateway products for sale of other products and services. Customers will have easier access to products from competitors for financial services and hence provide them with the ability to choose providers who offer better quality and service.

PSD2 also presents opportunities to banks to extend their reach by providing Account Information Services and Payment Initiation services. Banks can offer PIS services to merchants to directly transfer funds from the customer accounts, disintermediating the card schemes. They have the potential to charge a service fee for these services, which opens up a new revenue stream. Banks that have already implemented modern banking solutions, with secure access to API gateways and digital platforms, will be able to monetise their investment to offer additional services under PSD2.

3.1 Impact on banks acting as Payment Service Providers

PSD2 has a number of provisions which impact banks providing payment services. Some of them are detailed below.

3.1.1 Transparency of Payment Services

PSD2 mandates that explicit information on the terms and conditions of the service should be provided upfront when the payment is initiated and the payer should agree to the terms before the payment is executed. To enable customers to choose the payment service provider, the directive mandates provision of information on maximum execution time, all charges with breakdown and exchange rate (actual or reference) applicable for the payment order at payment initiation, upfront.

After receipt of the payment order, the payer's PSP should provide the transaction amount, all charges payable by the payer with breakdown, actual exchange rate, date of receipt of payment order and the debit value date.

Similarly, after execution of a payment, the payee should be provided with details of the payment including payment amount, all charges payable by the payee with breakdown, exchange rate (actual) and credit value date.

As per existing rules, Payer and Payee will pay for charges levied by their payment service providers, for transactions, where both PSPs are in member states. Also, a breakdown of the charges deducted should be provided.

3.1.2 Payments coverage

PSD2 has widened the scope of its applicability to include "one-leg-out" (OLO) payments, in any currency. They apply to payments initiated and ending in all the 28 EEA countries + Iceland, Liechtenstein, Norway. In the previous directive, these transactions were exempt from PSD.

Payments in a currency that is not of the currency of a Member State, which does not involve any currency conversion should be credited to the Payee, on the same business date of receipt of funds in the Payee PSP's account. However, PSPs are not bound by this rule, if a currency conversion is involved for a currency other than a Member state currency.

PSPs will still be allowed to deduct charges from the payment amount for OLO payments.

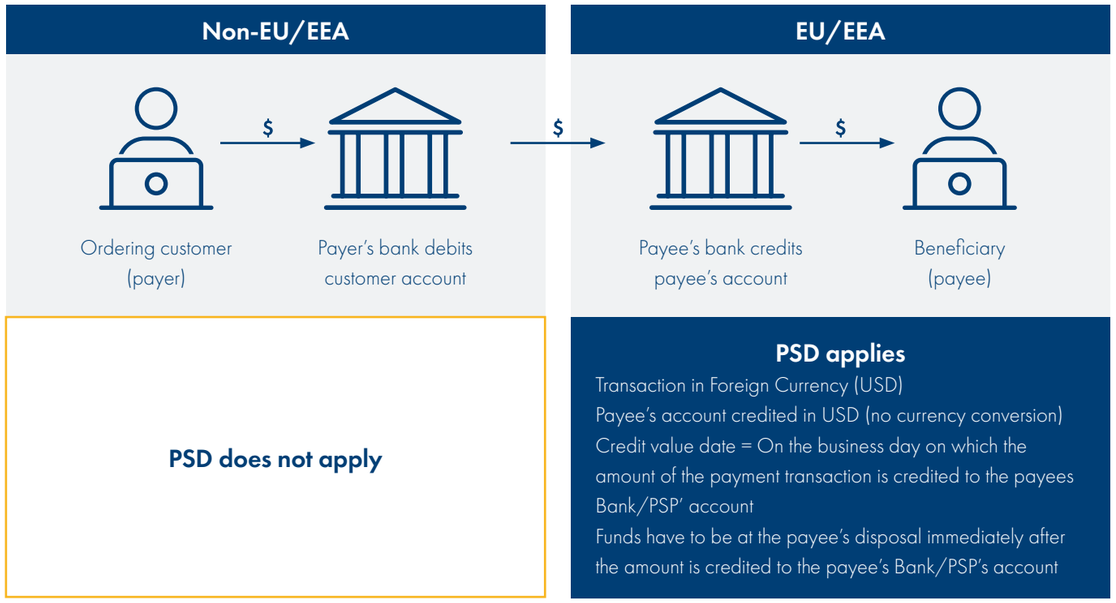


Figure 1: One Leg Out (OLO) Foreign Currency Payment under PSD2

Payments between PSPs in member states involving any currency other than a Member state currency, should follow the value dating rules. Payer and Payee shall pay for the charges levied by his payment service provider.

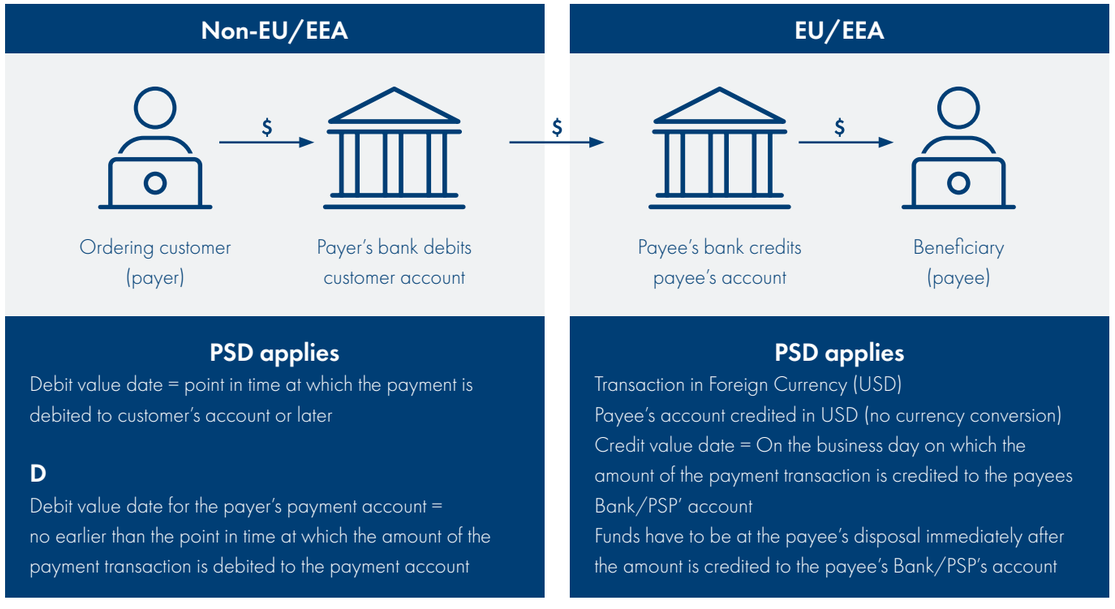


Figure 2: Payment within EU/EEA –Other than Member State Currency under PSD2

Removal of the exemptions for foreign currency payments will result in fall in service income from such payments and banks have to explore new opportunities presented by PSD2 to enhance their income.

3.1.3 Payment Initiation Services

PSD2 opens up the market for Third Party Providers (TPPs), offering Payment Initiation Services (PIS). 'Payment initiation service' means a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider. Authorised payment institutions can service customers as "Payment Initiation Service Providers (PISPs)".

PISPs will be allowed to communicate securely with the Customer's bank and seek information required for payment initiation. They will use software to link the merchant's website or app with the Customer's bank for initiating payments.

Given below is another example of a Payment Initiation service where the merchant goes through a PISP (say, a large bank), which provides service to collect money directly from the Customers' bank.

Already, there are several operators in the market providing such services, including e-commerce and m-commerce platforms, telecom or information technology networks which handle a huge volume of payment traffic, with no regulation, increasing the risk for consumers.

With PSD2, these institutions will be registered and supervised to enhance customer protection. EBA is seeking to drive competition and innovation through TPPs while ensuring that there is adequate customer protection.

E-Commerce and M-Commerce PISPs can now access customer information to execute payment transactions without entering into bi-lateral agreements with the Account Servicing Bank. This introduces a level playing field for these players and will result in stiff competition to traditional banks acting as Payment Service Providers.

On a strategic level, Banks need to consider potential changes to products and services offered to their customers. They should start looking to moving from being just Payment processors to payment acquirers.

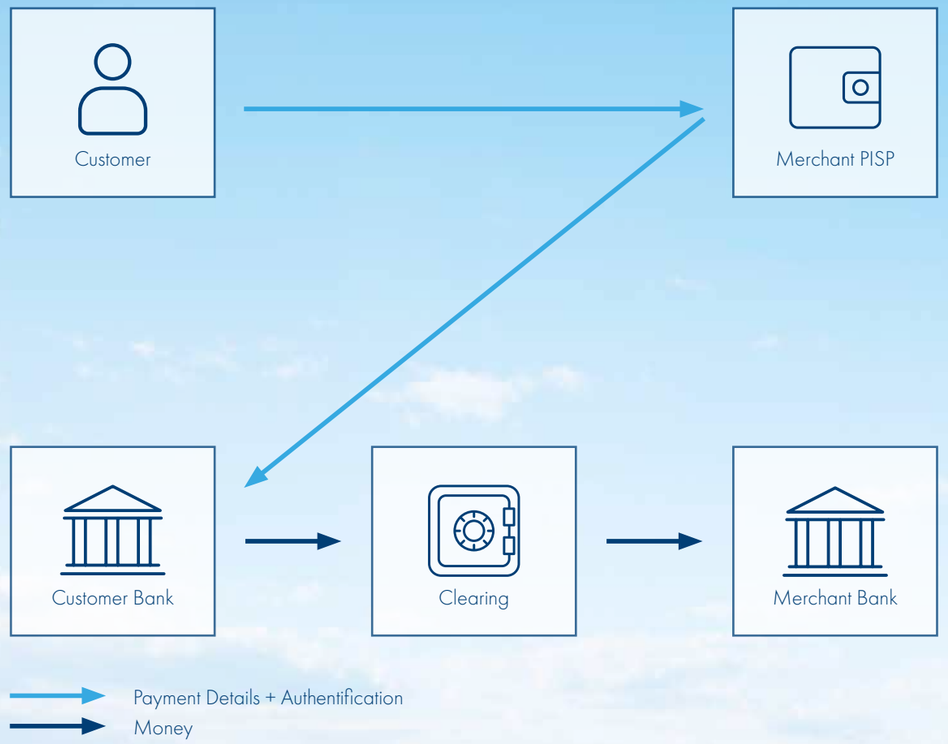


Figure 3: Payment Initiation Service – Credit Transfer

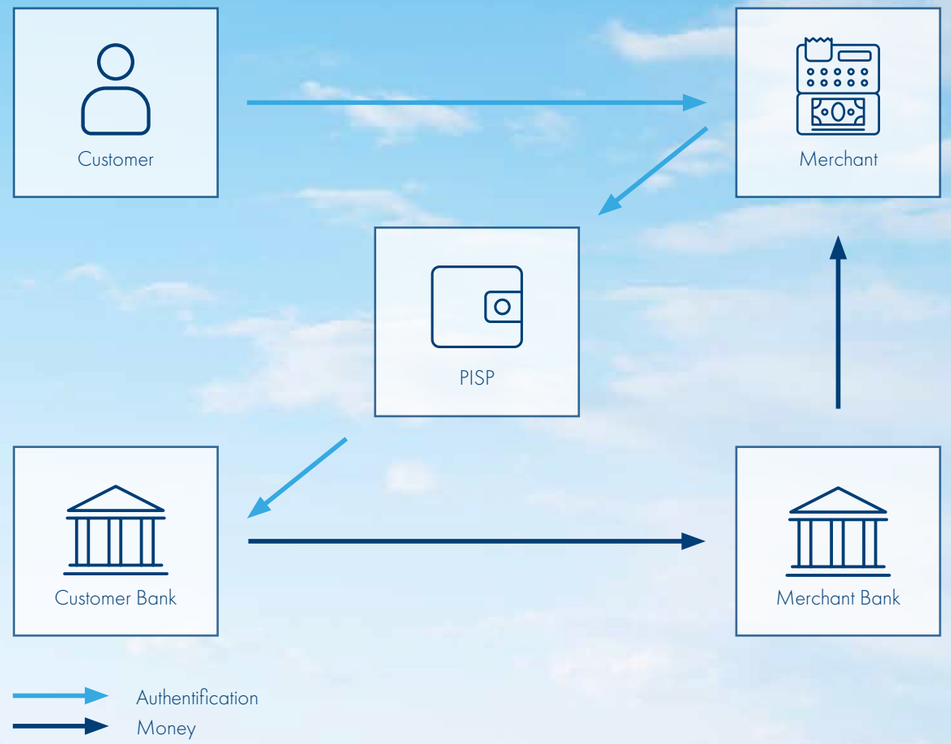


Figure 4: Payment Initiation Service – Through PISP

3.2 Impact on Banks acting as Account Servicing Institutions

PSD2 opens up the payments market to TPPs who can offer Account Information Services (AIS) and Payment Initiation Services (PIS). Such third parties offering payment services authorised to act as "Payment Institutions" as per the guidelines issued by EBA, are allowed to access account information without the existence of bilateral agreements with the Account Servicing Bank. Account Servicing Banks are mandated to provide such information to these TPPs.

3.2.1 Access to Accounts (XS2A)

TPPs can offer Account information services which aggregate information on one or several accounts held with one or several account-servicing PSPs and present that information to the account owner in a consolidated way. Banks have to provide open access to account information to all authorised TPPs, requesting account information via standard APIs.
Industry expert Dr. Michael Salmony, Executive Advisor at Equens SE, sees XS2A as an opportunity for banks, providing such access is controlled through standard interfaces/platforms, similar to the App-Store and Google-Play models of Apple and Google, with contracts in place that clarify the liability partitions between banks and TPPs. Since security is a key issue in payments, he rallies his case for "Controlled Access to Payment Services" (CAPS). CAPS is a proposal for the Regulatory Technical Standards (RTS) and enables us to plan development and implementation of the APIs.

PISPs can also seek information required for payment initiation, account verification and sufficient funds check, via APIs from the Customer's bank.

Banks face increased costs in implementing interfaces (APIs) for providing access to TPPs which is mandated under PSD2.

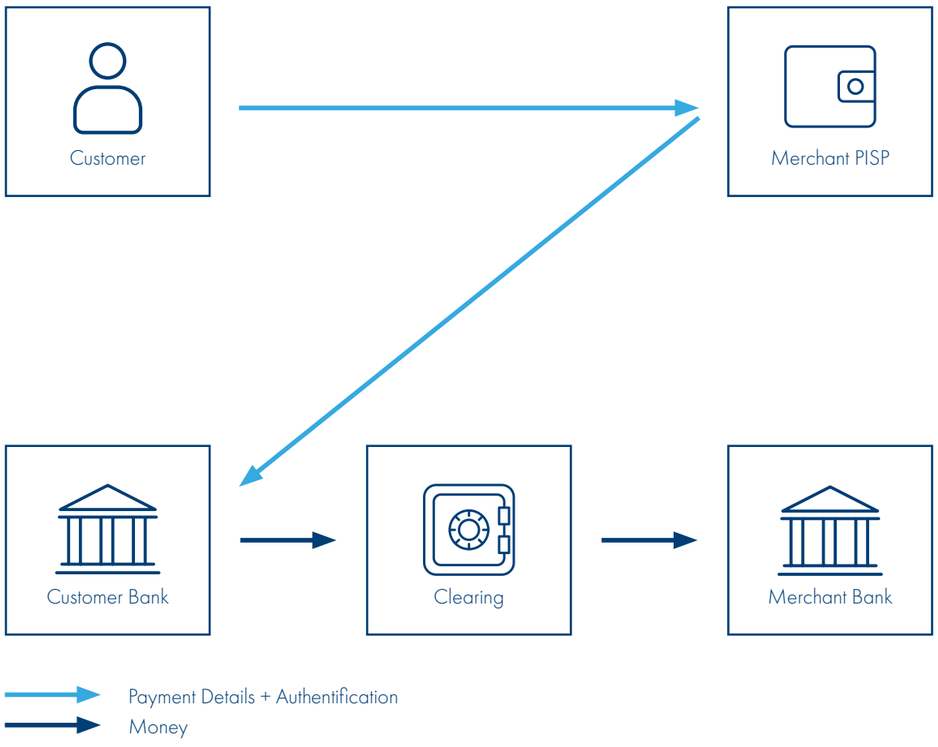


Figure 3: Payment Initiation Service – Credit Transfer

3.2.2 Customer Authentication and Security

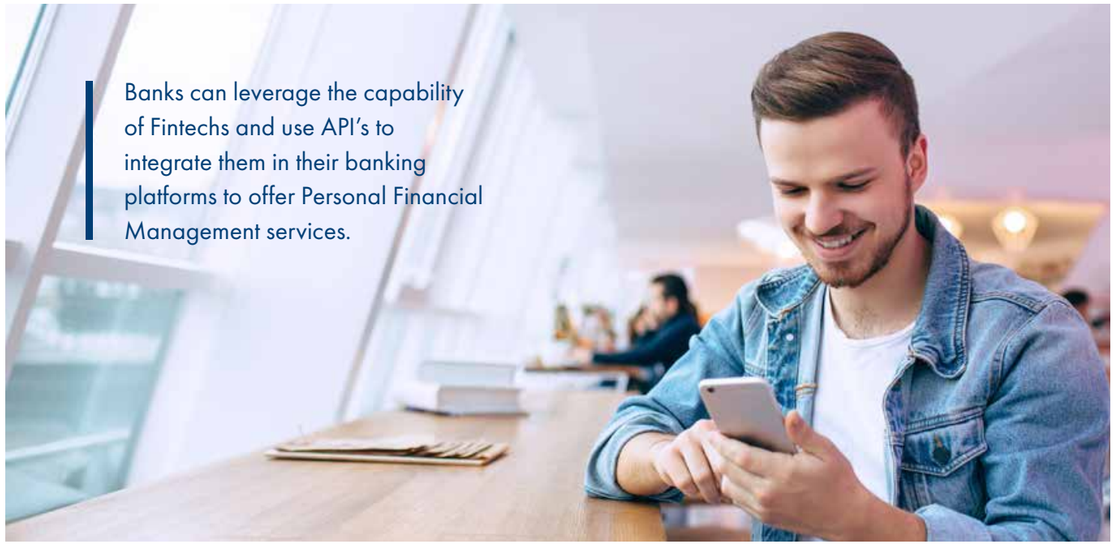
As banks should provide access to account and balance information freely to TPPs via open APIs, it becomes imperative to transmit such information securely to prevent fraud and illegal use of sensitive and personal data. One of the key provisions of PSD2 is to enforce requirements for strong (2-factor) customer authentication and security measures to protect the confidentiality and integrity of personalised security credentials of the payment service users. EBA is mandated to publish Regulatory Technical Standards (RTS) on authentication and communication.

While EBA will come up with the "common" and "open" standards for communication and authentication, OAuth is a widely used standard that provides a simple and secure mechanism for users to authenticate themselves, and authorise how their data can be shared. It allows a user to initiate sharing of their personal data between organisations without sharing their login credentials. It allows to limit access to user's data via APIs and provides users to authorise the terms of access.

TPPs providing Payment Initiation Services and Account information services are likely to use OAuth for authentication and access to customer information. Customers can directly login to their bank via internet banking and authorise access to a third party for access to specific information, relating to the transaction. Customers can also revoke access to share data with the third party providers, whenever they choose.

Open access to customer information via APIs, can potentially have different levels of authentication depending on the type of service; account information services which provide third party APIs "read only" access could be allowed used using OAuth and gaining user's consent to share data, while the ability to initiate payments, which requires write access, could involve multi-factor authentication.

Account Servicing Banks should have the right IT infrastructure to provide secure access to account and balance information, as mandated by PSD2.



3.3 Opportunities to Banks from PSD2

Banks can act as aggregators and offer "Account Information Services" to their customers and provide Personal Financial Management (PFM) services. Banks can leverage the capability of Fintechs in this space and use API's to integrate them in their banking platforms to offer such services. Premium services and products, based on data analytics, can be built on top of these platforms.

As access to account information for payment services is opened up, banks also can extend their reach in Retail Payments by extending their services as PISPs. Implementing a flexible IT architecture which will allow for extension of services beyond just providing access to account information is key for making the transition. Instead of being pure play payment processers, banks can move up the value chain by offering online Payment Initiation services from their Banking portals. Some banks have already started offering such services through Payment Wallets.

How to Prepare for PSD2?

4

Banks need to prepare themselves both at strategic and operational levels, to implement PSD2. This document suggests solutions to address some of the challenges and opportunities described above for Temenos prospects and customers acting as Payment Service Providers and Account Servicing Institutions.

4.1 Transparency of Payment Services

Payment application used for Payment initiation (in the Channels) should provide the ability to display to the payer, before execution of the payment, payment currency and amount, max execution time, date of receipt of order and Debit Value Date for the payment, exchange rate (actual or reference), if currency conversion is involved, and breakdown of charges payable by the payer. Payment should be executed upon receiving confirmation/consent from the payer. After execution, it should be possible to provide confirmation of execution of the payment with details of end to end charges, actual exchange rate, execution time and value date.

Similarly, the payment application used for execution of the payment, should provide to the payee, details of payment amount, currency credit value date, actual exchange rate applied and charges with breakdown.

Temenos Payment Solutions (Temenos Payment Order, Temenos Payment Suite and Funds Transfer) which provide front office payment initiation and mid/back office payment execution solutions, will be enhanced to provide additional payment information before and after execution of the payment, as mandated in the revised Payment Services Directive. Additional information for payment initiation will be available for display in the Temenos Channel solutions for internet and mobile banking.

4.2 Payments coverage

While executing payments, the payment application should have the ability to identify the country of origin (ordering bank/payer) of the payment and the destination (payee/beneficiary bank) country and apply the following rules:

If both payment origination and destination countries are within EU/EEA member states, then:

- Payment should be processed and credited to the payee by the end of the following business day of the receipt of the payment order from the payer. Payer's PSP needs to ensure that funds are credited to the payee's PSP next day and the payee's PSP should credit the payee on the date of receipt of funds. This is applicable for domestic payments in any member state currency, payments with one currency conversion between Euro and member state currency and cross border payments in Euro.

- Charges are shared by the Payer and Payee, i.e. payer pays for the charges levied by his PSP and payee pays for the charges levied by his PSP.

- Full payment amount should be transferred i.e. charges should not be deducted from the payment amount transferred. However, if the PSP has an agreement with the payee, charges can be deducted from the transaction amount and the PSP should provide a complete breakdown of the charges deducted from the payment amount. For payments executed in non-member state currencies, PSPs are allowed to deduct charges from the amount transferred.

- For OLO payments, when only the debit leg (origination country) of the payment is EU/EEA and the destination country is outside the EU/EEA, the payer should be debited only after the receipt of the payment order. Debit value date is the date of receipt of the Payment Order. If the payment is received on a non-working day, the debit value date shall be the next working day. This is applicable for payments in all currencies.

- In respect of OLO payments with only the credit leg (destination country) of the payment is EU/EEA, the payee should be credited on the business day the funds are credited in the payee PSP's account. If the credit to the payee's PSP's account is on a non-business day, the funds should be made available to the payee no later than the following business day. This applicable for payments in any member state currency, with or without any currency conversion and payments in non-member state currencies, with no currency conversion.

4.3 Access to accounts (XS2A)

Under PSD2, Banks servicing customer accounts should have the ability to provide access to account information sought by PISPs and AISPs. Information sought via APIs can include Payment User Verification, Account Verification, Sufficient Funds check and Balance Information. Account Servicing institutions are mandated to transfer such information securely with 2-factor customer authentication through market standard APIs.

Any request for information would only be accepted from a TPP that had been regulated by the banking authorities and where the customer has an agreement in place with a PISP or AISP. For this reason, any request for account information will need to be validated as follows:

- The AISP or PISP is present on the list of authorised TPPs
- The customer has an agreement in place with the PISP or AISP

So there needs to be a process in place as follows:

- The customer signs up with the TPP
- This is communicated to the Account Servicing Bank
- The Account Servicing bank need to get verification from the customer before the account information is flagged as being available at the TPP

Temenos frameworks provide reliable, secure and efficient access to data that we can expose through APIs, once the standard validation checks have been successful. EBA are mandated to define the RTS (Regulatory Technical Standards) in 2016. Once the RTS has been formally defined, our products will allow us to produce and package APIs that we will be able to offer/license to the Temenos customers (banks) to fulfil their access to accounts regulatory obligations under PSD2.

4.4 Customer Authentication and Security

Banks should implement 2-factor authentication for communication with TPPs.

Temenos Channels implement 2-factor user authentication, PKI authentication based on client/user certificates and storage and validation of digital signatures.

We believe that existing customer authentication and security protocols used by Temenos Channels already provide strong customer authentication and security. Once the RTS around authentication and communication is available, they will be reviewed to confirm the access to Temenos solutions complies with the standards.

Temenos will use OAuth 2.0 for authentication and authorisation.

4.5 Account Information Services

PSD2 defines "Account information service' as an online service to provide consolidated information (balance, transaction history) on one or more payment accounts held by the Payment Service User (PSU) with either another payment service provider or with more than one payment service provider. Banks have reputation and trust of customers and hence can act as online account aggregators, by monetising the investment on providing access to TPPs to account information via APIs.

Banks can host such information in the Temenos Channel Banking solution and integrate it in the Single Customer (3600) View of their customers. The Channel Banking solution of Temenos uses the Temenos Interaction Framework, which offers a platform to create OData Services (APIs) through a design time tooling and publish them in different media type formats i.e. atom-xml, hal+JSON for a truly multichannel user agents (mobile, tablets, desktop) experience. The architecture neatly de-couples the backend with the services needed for UI (user agent) thereby offering major benefits for banks and new entrants (TPPs, FinTech providers) to grow at their own pace. Temenos already uses Interaction Framework for creating banking APIs for read-only data i.e. to view an account balance, transaction list, etc. Temenos will offer the requested APIs under PSD2 along with the flexibility to create new ones using the design time tooling feature of Interaction framework.

4.6 Payment Initiation Services

Banks can offer Payment Initiation Services using the Temenos Payment Order solution. Temenos Payment Order can be used to initiate payments in Internet, Mobile and Branch channels and the solution is completely inter-operable across channels.

Temenos Payment Order deployed in Temenos frameworks, can request access to external (not within the processing Bank, TPP) account information via APIs and execute the payment orders.

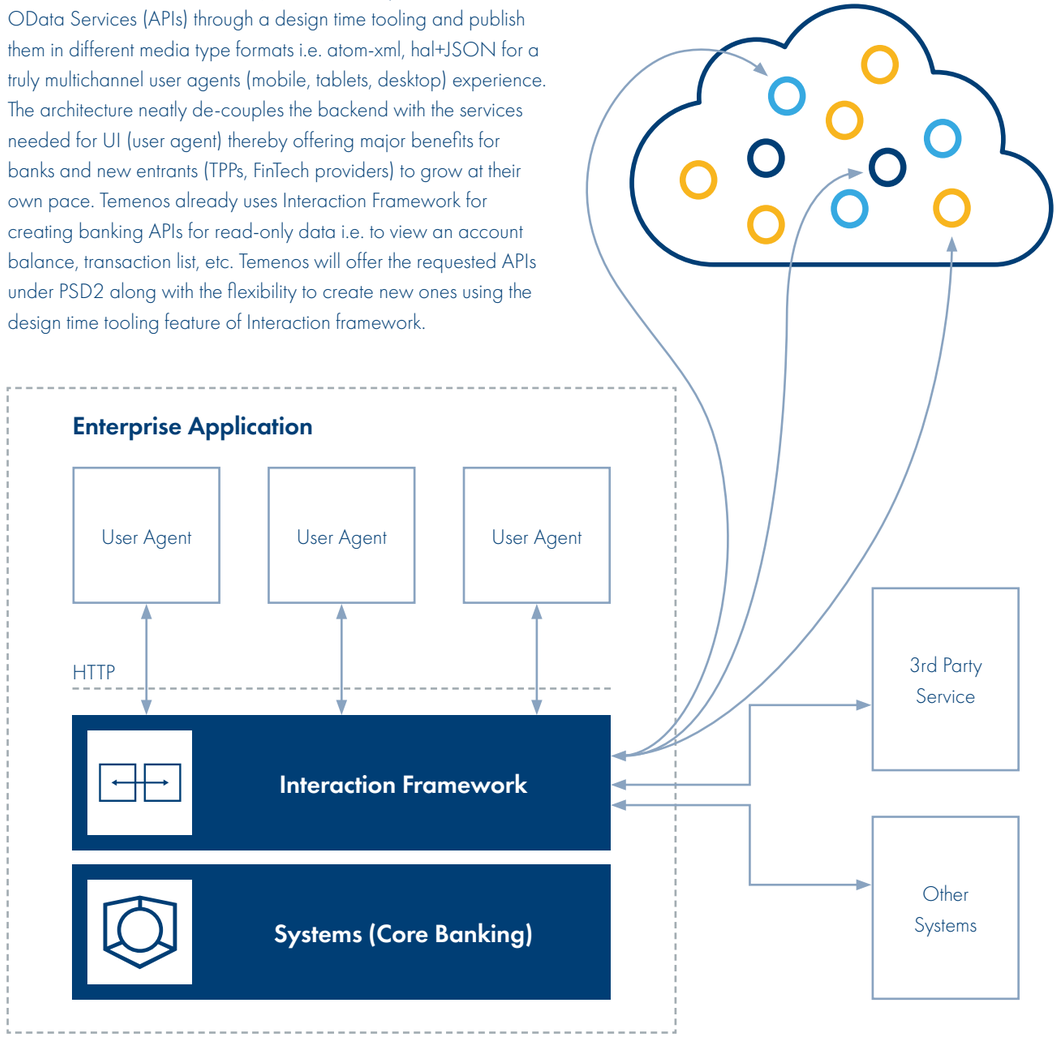


Figure 6: Temenos Interaction Framework

Temenos Response to PSD2

5

Banks can provide plugins/extensions for Payment Initiation services which can be integrated by merchants on their online/mobile channels to enable buyers to make payments for online purchases. Banks can charge a fee from the merchants for such services. Temenos response to PSD2:

1 **Transparency of Payment Services** - Temenos Payment Solutions (Temenos Payment Order, Temenos Payment Suite and Funds Transfer) which provide front office payment initiation and mid/back office payment execution solutions, will be enhanced to provide additional payment information before and after execution of the payment, as mandated in the revised Payment Services Directive. Additional information for payment initiation will be available for display in the Temenos Channel solutions for internet and mobile banking.

2 **Payments Coverage** - Temenos Payment solutions will be enhanced to allow execution of payments as per the new rules, through configuration.

3 **Access to Accounts** - Temenos frameworks provide reliable, secure and efficient access to data that we can expose through APIs, once the standard validation checks have been successful. EBA are mandated to define the RTS (Regulatory Technical Standards) in 2016. Once the RTS has been formally defined, our products will allow us to produce and package APIs that we will be able to offer/license to the Temenos customers (banks) to fulfil their access to accounts regulatory obligations under PSD2.

4 **Customer Authentication and Security** - Temenos Channels implement 2-factor user authentication, PKI authentication based on client/user certificates and storage and validation of digital signatures. Once the RTS around authentication and communication is available, they will be reviewed to confirm the access to Temenos solutions complies with the standards.

5 **Account Information Services/Payment Information Services** - Temenos will offer the requested APIs under PSD2 along with the flexibility to create new ones using the design time tooling feature of Interaction framework.

Conclusion

6

PSD2 aims to bring online payment service providers such as PayPal, PayMill etc. and PAYM type mobile payment companies under the regulation. It brings greater transparency to the products and services offered by Payment Service providers.

Competition is encouraged by allowing access to third party providers to account information to provide Payment Initiation and Account Information services. It also provides opportunity for traditional and new players in the financial services space to use digital platforms to capitalise on the opportunities offered under PSD2.

PSD2 versus PSD

7

	Revised Payment Services Directive (PSD2)	Payment Services Directive (PSD)
Effective Date	13th January 2018	In full force from 1st November 2009
Currency	Any currency	Euro and non-euro currencies of EU/EEA
Amount	No limit on amount	No limit on amount
Geographical scope	EU/EEA, Iceland, Liechtenstein, Norway (plus Switzerland also expected in 2017/18)	EU/EEA
Transactions and Services	Card payments, direct debits and credit transfers in the EU/EEA, Iceland, Liechtenstein, Norway (plus Switzerland) at national and cross-border level Cash deposits and withdrawals M-payments and e-payments Money remittances Payment initiation services and Account information services	Card payments, direct debits and credit transfers in the EU/EEA at national and cross-border level Cash deposits and withdrawals M-payments and e-payments Money remittances
Amounts Transferred and received	Charges should not be deducted from the amount transferred for payments in member state currencies. Full payment amount should be transferred. Charges can be deducted from the payment amount received by the payee, with prior agreement. Actual payment received and charges deducted should be provided in the confirmation to the payee.	Charges should not be deducted from the amount transferred for payments in member state currencies. Full payment amount should be transferred. Charges can be deducted from the payment amount received by the payee, with prior agreement. Actual payment received and charges deducted should be provided in the confirmation to the payee.

	Revised Payment Services Directive (PSD2)	Payment Services Directive (PSD)
Execution Time	Process payments by D+1 max. (D = point in time of receipt) One additional day allowed for paper initiated transactions D+4 possible for certain intra-Union payments	Process payments by D+1 max. from 2009 (D = point in time of receipt) Up to D+3 possible until 1 st January 2012 only if there is an agreement between payment service provider and ordering customer One additional day allowed for paper-initiated transactions D+4 possible for certain intra-Community payments
Value Date	For the payer/ordering customer – Debit Value Date is date of receipt of payment order. If the payment is received on a non-working day, then value applied will be next Business Day. Rule is applicable for payments in any currency. For payee/beneficiary – Credit Value date is the date of receipt of funds in the Payee's bank account. This applies to payments in any currency involving no currency conversion and payments in member state currencies, involving a currency conversion	For the payer/ordering customer – Debit Value Date is date of receipt of payment order. If the payment is received on a non-working day, then value applied will be next Business Day. Rule is applicable for payments in member state currencies. For payee/beneficiary – Credit Value date is the date of receipt of funds in the Payee's bank account. This applies to payments in member state currencies.
Information (Transparency)	Stipulates minimum information requirements from payment service provided to customer. Also, makes it mandatory to disclose the terms and conditions of service upfront (execution time, exchange rate and end to end charges) to the payer before execution of the payment and execute upon receiving consent.	Stipulates minimum information requirements from payment service provided to customer.

PSD2 Exclusion List

8

The directive does not apply to the following types of payments:

1. cash payments directly from payer and payee; with no intermediary intervention
2. certain types of cash payments, including cash to currency exchange where funds not held in a payment account, transport of bank notes and coins, cash collection by non-profit organisations, etc.
3. paper based payment transactions including paper cheques, paper drafts, vouchers, traveller's cheques; postal money orders etc.
4. payment transactions in a settlement system amongst payment service providers, settlement agents, clearing houses, central banks and other participants
5. payment transactions related to securities asset servicing such as distribution of dividends, income, redemption or sale of securities carried out by investment services firms, asset management firms, credit institutions etc.
6. services provided by technical service providers in managing infrastructure (devices, networks) used for payment services.
7. services based on specific payment instruments used only in a limited way to acquire a limit range of goods or services (Store Cards, Fuel Cards, Meal Vouchers, Social Security Benefit cards, etc.)
8. payment transactions by a provider of electronic communication networks or services for purchase of digital content and voice based services, charitable activity and purchase of tickets; where the value of a single payment transaction does not exceed EUR 50 and the cumulative value of the payment transactions does not exceed EUR 300 per month
9. payment transactions amongst undertakings (parent and subsidiaries of the same parent) with no intermediary intervention.
10. cash withdrawal services in ATMs by providers acting on behalf of card issuers; which are not party to the framework contract with the customer withdrawing money from the payment account. However, the transparency rules relating to information on charges applicable for such cash withdrawals.

Glossary

9

Abbreviation	Term	Definition
AIS	Account Information Services	An online service to provide consolidated information on one or more payment accounts of a Payment Service User (PSU) held at one or more AS PSPs.
AISPs	Account Information Service Providers	An AISP acts as an aggregator of data relating to a Payment Service User's accounts held at one or many different AS PSPs.
AS PSPs	Account Servicing Payment Service Providers	A traditional type of Payment Institution with which a Payment Service User (PSU) holds an account and from which the PSU issues payment orders. Every AS PSP must register under PSD2 as a Payment Institution unless it is a "Credit Institution" under Regulation (EU) No 545/2013 of the European Parliament and of the Council.
EC	European Council	
EEA	European Economic Area	
CAPS	Controlled Access to Payment Services	CAPS is a proposal for the Regulatory Technical Standards (RTS) from Equens. It enables us to plan development and implementation of the APIs.
OAUTH 2.0	Open Authorisation	OAuth is an open standard that provides a simple and secure mechanism for users to authenticate themselves, and authorise how their data can be shared. It allows users to share personal and financial data between organisations without sharing their login credentials.
OLO	One-Leg Out Payment	A payment where one leg of the transaction happens outside the EU/EEA.

Abbreviation	Term	Definition
PIS	Payment Initiation Services	Service to initiate a payment order at the request of the Payment Service User (PSU) with respect to a payment account held at another payment service provider.
PISPs	Payment Initiation Service Providers	PISPs initiates payments on behalf of the PSU who grants permission to do so. PISPs create a software link between the website or app of the merchant and the online banking platform of a payer's bank in order to initiate the payment. They are made available as an option on a merchant's website.
PSD2	Revised Payment Services Directive adopted by European Parliament and EU Council	
PSPs	Payment Service Providers	Traditional Payment Service Providers (PSPs) such as banks and financial institutions and providers that offer online services for accepting electronic payments by a variety of methods including credit/debit cards, real time payments, credit transfers and direct debits.
PSU	Payment Service User	An individual or corporate entity who has one or more accounts with an AS PSP.
RTS	Regulatory Technical Standards	A set of technical standards to be developed by EBA for implementation of PSD2. One particular Technical standard, on strong customer authentication and secure communication, is key to providing access to information and accounts.
TPPs	Third Party Providers	TPPs are Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs) regulated under PSD2. They enable payment initiation and account access on behalf of customers.
XS2A	Access to Accounts	

Examples 10

10.1 Example 1: Fidor Bank - APIs to Access Account Information and Initiate Payments

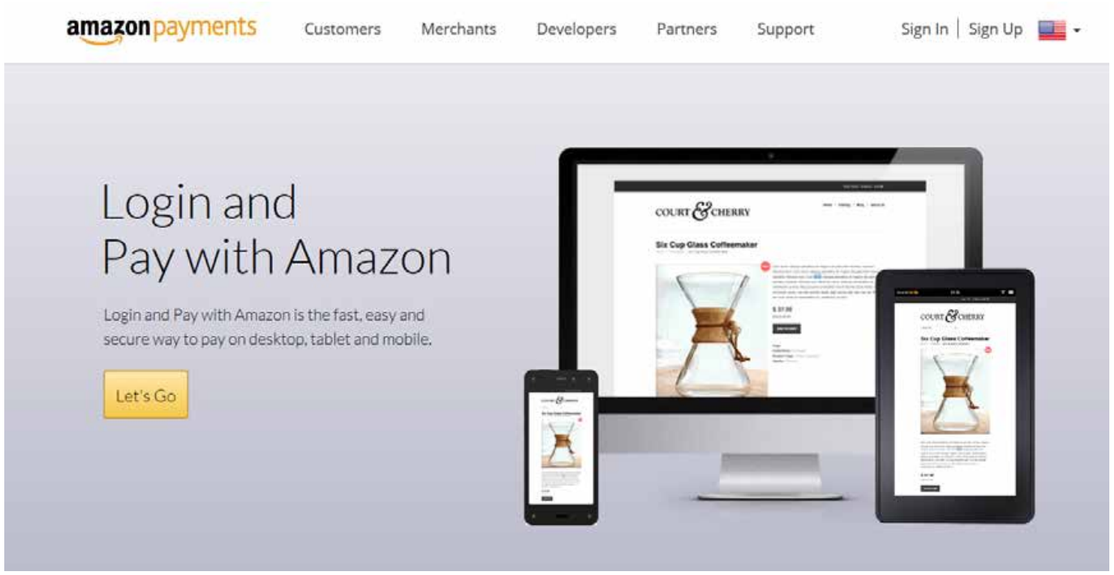
How it works for bank customers developing applications using APIs offered by Fidor:

1. Login to online bank account
2. Access Fidor Application Manager
3. Add an Application (to use the API). In order to use the API, customer has to tell Fidor
   a. Name
   b. Purpose and
   c. Technical information of the application which accesses the API
4. Use the range of APIs offered by Fidor Bank such as
   a. Get Account information
   b. Initiate individual and batch SEPA Payments – Credit transfers
   c. Initiate Direct Debits
5. Test the application in the API sandbox
6. Select access permissions for the application
   a. Access own account data
   b. Access account details/data of other account holders (will require account holders to authorize access to their respective accounts)

How it works for the account holder using application:

1. Directs account holder to Fidor web page
2. Asked to enter user name and password
3. If application (app), is not previously approved, asks the account holder to confirm that the app is allowed to access their account within the given scope
4. Account holder returns back to the application

Application will make calls via API and displays the results. Allows integration with e-commerce store for tracking payments against orders and initiating credit transfers and direct debits, apart from accessing account information. Fidor Bank charges a monthly fee from the customer using the APIs from their applications.



10.2 Example 2: Amazon payments – Payment Initiation Service Provider

How it works for Merchants:

1. Integrate readily available Amazon payments extensions/ plugins with eCommerce Platform or develop/deploy applications which integrate with amazon payments.
2. Pay with Amazon icon is integrated in the ecommerce portal/store
3. Customers can choose to "Pay with Amazon" when they checkout their orders
4. Customers enter their Amazon username and password
5. Customers select shipping address and payment method
6. Customers review and submit their orders
7. Payment is executed via the chosen method.

temenos.com

About Temenos

Temenos AG (SIX: TEMN), headquartered in Geneva, is the world's leader in banking software, partnering with banks and other financial institutions to transform their businesses and stay ahead of a changing marketplace. Over 3,000 firms across the globe, including 41 of the top 50 banks, rely on Temenos to process both the daily transactions and client interactions of more than 500 million banking customers. Temenos offers cloud-native, cloud-agnostic front office and core banking, payments, fund management and wealth management software products enabling banks to deliver consistent, frictionless customer journeys and gain operational excellence. Temenos customers are proven to be more profitable than their peers: over a seven-year period, they enjoyed on average a 31% higher return on assets, a 36% higher return on equity and an 8.6 percentage point lower cost/ income ratio than banks running legacy applications.

Learn More

To find out how Temenos can help with your digital banking needs, contact sales@temenos.com or visit us at www.temenos.com

TEMENOS

THE BANKING SOFTWARE COMPANY